Air Force Institute of Technology
AFIT Scholar

Theses and Dissertations Student Graduate Works

3-16-2009

Mitigating Insider Sabotage and Espionage: A Review of the United States Air Force's Current Posture

Erika C. Leach

Follow this and additional works at: https://scholar.afit.edu/etd

Part of the Databases and Information Systems Commons, and the Information Security Commons

Recommended Citation

Leach, Erika C., "Mitigating Insider Sabotage and Espionage: A Review of the United States Air Force's Current Posture" (2009). *Theses and Dissertations*. 2545.
https://scholar.afit.edu/etd/2545

This Thesis is brought to you for free and open access by the Student Graduate Works at AFIT Scholar. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of AFIT Scholar. For more information, please contact richard.mansfield@afit.edu.

MITIGATING INSIDER SABOTAGE AND ESPIONAGE:

A REVIEW OF THE UNITED STATES AIR FORCE'S CURRENT POSTURE

THESIS

Erika C. Leach, Captain, USAF

AFIT/GIR/ENG/09-05

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENG/09-05

MITIGATING INSIDER SABOTAGE AND ESPIONAGE: A REVIEW OF THE UNITED STATES AIR FORCE'S CURRENT POSTURE

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Erika C. Leach, BA

Captain, USAF

March 2009

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT/GIR/ENG/09-05

MITIGATING INSIDER SABOTAGE AND ESPIONAGE:
A REVIEW OF THE UNITED STATES AIR FORCE'S CURRENT POSTURE

Erika C. Leach, BA
Captain, USAF

Approved:

//SIGNED// 13 March 2009
Robert F. Mills (Chairman) Date

//SIGNED// 13 March 2009
Michael R. Grimaila (Member) Date

//SIGNED// 16 March 2009
Gilbert L. Peterson (Member) Date

AFIT/GIR/ENG/09-05

Abstract

The security threat from malicious insiders affects all organizations. Mitigating this problem is quite difficult due to the fact that (1) there is no definitive profile for malicious insiders, (2) organizations have placed trust in these individuals, and (3) insiders have a vast knowledge of their organization's personnel, security policies, and information systems.

The purpose of this research is to analyze to what extent the United States Air Force (USAF) security policies address the insider threat problem. The policies are reviewed in terms of how well they align with best practices published by the Carnegie Mellon University Computer Emergency Readiness Team and additional factors this research deems important, including motivations, organizational priorities, and social networks.

Based on the findings of the policy review, this research offers actionable recommendations that the USAF could implement in order to better prevent, detect, and respond to malicious insider attacks. The most important course of action is to better utilize its workforce. All personnel should be trained on observable behaviors that can be precursors to malicious activity. Additionally, supervisors need to be empowered as the first line of defense, monitoring for stress, unmet expectations, and disgruntlement. In addition, this research proposes three new best practices regarding (1) screening for prior concerning behaviors, predispositions, and technical incidents, (2) issuing sanctions for inappropriate technical acts, and (3) requiring supervisors to take a proactive role.

Acknowledgments

I would like to thank my thesis advisor, Dr. Mills, for all the guidance and knowledge he shared. His wisdom was essential as I made my way through this research venture. I would also like to express my gratitude for the time that my other committee members, Drs. Grimaila and Peterson, invested into this project. Additionally, I could not have completed this venture without the research and expertise of the Carnegie Mellon University Computer Emergency Readiness Team technical staff. I very much appreciated their generosity in inviting me to their research facility and taking the time to share their experience and advice.

I would lastly like to thank my family and friends for their endless love and support. They were always there to listen to my frustrations and rejoice in my accomplishments.

Erika C. Leach

Table of Contents

Page

Abstract……………………………………………………………………........ iv

Acknowledgments…………………………………………………………........ v

Table of Contents…………………………………………………………………. vi

List of Figures…………………………………………………………………….. x

List of Tables……………………………………………………………………... xii

I. Introduction……………….……………………………………………... 1
- 1.1 Overview……………..…………………………………………………… 1
- 1.2 Research Objectives……………………..…………………….............. 3
- 1.3 Scope……...……………………..………………………………............. 4
- 1.4 Thesis Organization……………………………………………............ 5

II. Literature Review……………………...…………………………............ 7
- 2.1 Overview……….....…………….. 7
- 2.2 Factors in the Insider Threat Problem………....…………….................. 7
  - 2.2.1 Precursors of the Malicious Party………………..………................ 7
  - 2.2.2 Insider's Expectations…………….. 10
  - 2.2.3 Event Triggers……………………... 11
  - 2.2.4 Social Networks……….……... 11
  - 2.2.5 Insider Motivations………..……... 12
  - 2.2.6 Organizational Controls………….. 13
  - 2.2.7 Organizational Priorities…………... 15
  - 2.2.8 Organizational Trust………... 15
  - 2.2.9 Risk Management………... 16
- 2.3 Case Studies………... 19
- 2.4 Insider Threat Models………... 22
  - 2.4.1 Voltaire…….. 22
  - 2.4.2 Risk Predictor Model………... 23
  - 2.4.3. Multidiscipline Approach to Mitigating the Insider Threat……….... 24
  - 2.4.4. Logical Data Modeling………….. 25
    - 2.4.4.1 Background Information on Logical Data Modeling……... 25
    - 2.4.4.2 Structural Approach to Insider Computer Misuse Incidents.. 27
  - 2.4.5 System Dynamics Modeling………... 28
    - 2.4.5.1 Background Information on System Dynamics Modeling.. 28
    - 2.4.5.2 Insider Attack on an Information System………………… 31
    - 2.4.5.3 Insider IT Sabotage Model……………………………….. 31

Page

2.4.5.4 Espionage Model 33
2.4.5.5 Abstracted Common Model 37
2.4.5.6 Model of the Insider IT Sabotage Problem 40
2.5 Summary 40

III. Insider Threat Modeling 42
3.1 Overview 42
3.2 Logical Data Model 42
3.2.1 Entities of the Logical Data Model 43
3.2.1.1 Organization 43
3.2.1.2 Control 43
3.2.1.3 System 45
3.2.1.4 Insider 46
3.2.1.5 Psychological Profile 47
3.2.1.6 Legal Profile 47
3.2.1.7 Computer Use Profile 47
3.2.1.8 Social Profile 48
3.2.1.9 Economic Profile 48
3.2.1.10 Ideological Profile 48
3.2.1.11 Professional Profile 49
3.2.1.12 Event 49
3.2.1.13 Relationship 50
3.2.1.14 Motivation 51
3.2.1.15 Incident 52
3.2.1.16 Threat 52
3.2.1.17 Vulnerability 52
3.2.1.18 Likelihood 53
3.2.1.19 Impact 54
3.2.1.20 Risk 54
3.2.2 Relationships in the Logical Data Model 54
3.3 System Dynamics Model 57
3.3.1 Organizational Controls 58
3.3.2 Insider's Motivation to Commit Malicious Act 60
3.3.3 Relationships Between Insider’s Motivation and Organizational Controls 60
3.3.4 Incorporation of Risk Management 61
3.3.5 Feedback Loops 61
3.4 Selection of the Abstracted Common Model 63
3.5 Modification of the Abstracted Common Model 64
3.5.1 Insider Motivations 64
3.5.2 Organizational Priorities 65
3.5.3 Social Networks 68
3.6 Summary 70

Page

IV. Policy Review …………………………………………………………….…….. 71
- 4.1 Overview…………………….……………………………..……………….. 71
- 4.2 Methodology of the Policy Review………………………………………. 71
  - 4.2.1 Best Practices for Mitigating Insider Threat………………………... 77
  - 4.2.2 Variables of the Insider Threat Model for Sabotage and Espionage.. 83
- 4.3 Findings for Best Practices and Variables……………………………... 87
  - 4.3.1 Best Practice- "Institute periodic enterprise-wide risk assessments"……………………………………………………… 89
  - 4.3.2 Best Practice- "Institute periodic security awareness training for all employees"……………………………………………………….. 91
  - 4.3.3 Best Practice- "Enforce separation of duties and least privilege"….. 93
  - 4.3.4 Best Practice- "Implement strict password and account management policies and practices" ……………………………………………… 94
  - 4.3.5 Best Practice- "Log, monitor, and audit employee online actions. Collect and save data for use in investigations"…………………….. 96
  - 4.3.6 Best Practice- "Use extra caution with system administrators and privileged users" ………………………………………………… 98
  - 4.3.7 Best Practice- "Actively defend against malicious code"………….. 99
  - 4.3.8 Best Practice- "Use layered defense against remote attacks"………. 100
  - 4.3.9 Best Practice- "Monitor and respond to suspicious or disruptive behavior"……………………………………………………………. 100
  - 4.3.10 Best Practice- "Deactivate computer access following termination"……………………………………………………….. 101
  - 4.3.11 Best Practice- "Implement secure backup and recovery processes"……………………………………………………………. 102
  - 4.3.12 Best Practice- "Analyze current access control policies and practices; identify and evaluate options to mitigate insider threat risk"…….. 102
  - 4.3.13 Best Practice- "Clearly document insider threat controls"………... 103
  - 4.3.14 Variable- "Sanctions" (for inappropriate technical acts)…………. 103
  - 4.2.15 Variable- "Organization's Prioritization of Profit"………………... 104
  - 4.3.16 Variable- "Organization's Prioritization of Reputation"…………... 104
  - 4.3.17 Variable- "Organization's Trust of Insider"……………………….. 104
  - 4.3.18 Variable- "Insider Stress"………………………………………… 105
  - 4.3.19 Variable- "Stressful Event"……………………………………….. 105
  - 4.3.20 Variable- "Personal Predispositions"……………………….…….. 106
  - 4.3.21 Variable- "Negative Relationships with Co-Workers"……………. 106
  - 4.3.22 Variable- "Positive Relationships with Co-Workers"…………….. 107
  - 4.3.23 Variable- "Personal Needs"……………………………………….. 107
  - 4.3.24 Variable- "Detecting Concerning Behavior and Technical Actions"……………………………………………………...…….. 107
- 4.4 Recommendations for Better Mitigating Insider Threat…………………. 108
  - 4.4.1 Risk Management and Backup Plans……………………………… 108
  - 4.4.2 Limit Power of a Single Employee………………………………… 109

Page

4.4.3 Account Management………………………………………………. 110
4.4.4 Monitoring Online Actions………………………………………… 111
4.4.5 Creating Baselines……………………………………………….. 111
4.4.6 Training and Awareness…………………………………………. 112
4.4.7 Gaining Insight into Personality of the Insider……………………... 114
4.4.8 Role of the Supervisor…………………………………………….. 115
4.4.9 Documenting Insider Threat Controls……………………………..... 116
4.5 Additional Best Practices for All Organizations………………………….. 117
4.5.1 Screen for prior concerning behavior and technical actions, as well as personal dispositions……………………………………………... 117
4.5.2 Issue sanctions to employees for inappropriate technical acts……… 118
4.5.3 Require supervisors to take a proactive role………………………... 120
4.6 Summary ……………………………………………………………. 121

V. Conclusions……………………………………………………………….. 122
5.1 Summary of the Problem……………………………………………….. 122
5.2 Thesis Conclusions……………………………………………………….. 123
5.3 Impact of this Research…………………………………………………. 125
5.4 Possibilities for Future Research……………………………………….. 125

Appendix A: Detailed Policy Review ………………………………………… 128

Bibliography………………………………………………………………… 143

List of Figures

Figure Page

1. Cyber Event/Observable Taxonomy…………………………………………… 10
2. Example Risk Level Matrix……………………………………………………. 18
3. MAMIT…………………………………………………………………………… 24
4. Logical Data Model Example…………………………………………………...... 26
5. Logical Data Model Symbols……………………………………………………….. 27
6. System Dynamics Modeling Example ………………………………………… 29
7. Stock and Flow Symbols……………………………………….………….. 30
8. Stock and Flow Example……………………………………………………….. 30
9. Model of Insider Attack on an Information System.…………………………… 32
10. Insider IT Sabotage Model……………………………………………………… 34
11. Model Feedback Loops……………………………………………………….. 35
12. Espionage Model……………………………………………………………….... 36
13. Abstracted Common Model…………………………………………………….. 39
14. Model of the Insider IT Sabotage Problem…………………………………… 41
15. Insider Threat Logical Data Model…………………………………………… 44
16. Organization and Related Entities…………………………………………….. 45
17. Insider and Profile Entities……………………………………………………. 46
18. Insider and Related Entities…………………………………………………… 50
19. Incident and Related Entities…………………………………………………….. 51
20. Risk and Related Entities………………………………………………………… 53

Figure Page

21. Insider Threat System Dynamics Model……………………………………… 59

22. Insider Threat Model for Sabotage and Espionage……………………………. 66

23. Cyber Event/Observable Taxonomy…………………………………………... 75

24. Insider Threat Model for Sabotage and Espionage……………………………. 119

List of Tables

Table Page

1. Summary of Findings………………………………………………………….. 88

MITIGATING INSIDER SABOTAGE AND ESPIONAGE:

A REVIEW OF THE UNITED STATES AIR FORCE'S CURRENT POSTURE

I. Introduction

1.1 Overview

The security threat from malicious insiders is a substantial problem in all organizations today. In this research an insider is defined as someone who is or has been with the organization and can be from any of the following categories: employees, service providers, consultants, and contractors (CSO, 2007). Activities and methods used by insiders can vary from espionage to sabotaging an organization's network. According to *CSO* magazine's "2007 E-Crime Watch Survey," 26% of the security events occurring in that year were known or believed to be caused by insiders, compared with 58% being attributed to outsiders. Of the 671 security executives and law enforcement officials surveyed, 29% of them felt the greatest threat to cyber security came from insiders, compared to 41% who believed outsiders presented the greater risk (CSO, 2007). When comparing the cost of attacks, 34% of the respondents cited insider attacks as being the most damaging, compared to 37% choosing attacks from outsiders (CSO, 2007).

One of the reasons why the insider threat problem is so difficult to combat, as well as why these attacks can be so damaging, is because insiders are trusted by and have knowledge of the organization. Insiders have a huge advantage compared to outsiders by already knowing the organization's personnel, security policies, and information systems

(Mills et al., 2009). In addition, the organization has consciously decided to put trust in its employees and may even have subjected them to background checks and interviews.

In the case of former insiders, the trust may have been rescinded but these individuals retain their knowledge of the organization's functions, people, and processes. Non-disclosure agreements are often used to deter individuals from using that knowledge, but the risk exists nonetheless.

The vast majority of the respondents of the "2007 E-Crime Watch Survey" were more concerned about attacks than they were the previous year, and only 11% saw a decrease in the number of and financial loss from targeted attacks. Given these figures it is surprising that the results showed that the average spending on information technology and corporate security has decreased (CSO, 2007). Additionally, implementing appropriate security measures to prevent insider attacks does not appear to be a priority. The creation and use of background checks, account and password management policies, monitoring and auditing tools, and training and awareness programs all fell significantly in 2007 (CSO, 2007). Less than half of the respondents claimed to use the following essential security measures: security and account audits, employee monitoring, training and awareness programs, periodic risk assessments, reporting of misuse, and technically enforced separation of duty policies (CSO, 2007). In contrast, measures to prevent outside attacks, such as the use of firewalls, SPAM filtering, and anti-virus tools, were almost universally used (CSO, 2007).

It is important to note that even if an organization is not detecting malicious activity, it may still be occurring. This organization may not have sufficient controls in place as a result of the organization not having experienced an attack. Some organizations fall into a “trust trap” in which they cut back on security measures since they are not detecting any malicious activity and feel they can trust their employees (Moore et al., 2008). However, an attack can come at any time, with the attackers and methods of attack changing constantly. It can be difficult to know what mechanisms are successfully preventing insider attacks, but companies may find out the hard way if they cut back on security controls. With organizations primarily focusing their attention on attacks coming from the outside, the current security environment is very attractive to those insiders wishing to do harm.

1.2 Research Objectives

The purpose of this research is to analyze to what extent the United States Air Force (USAF) security policies address the insider threat problem. The policies are first examined using a set of best practices published by the Carnegie Mellon University Computer Emergency Readiness Team (CMU CERT) technical staff (Cappelli et al., 2006; Band et al., 2006). Specifically, the research analyzes if and how well the USAF security policies, as well as a few of the cornerstone Department of Defense (DoD) policies, implement these best practices.

Furthermore the policies are reviewed in terms of how well they addressed the variables in this research’s “Insider Threat Model for Sabotage and Espionage.” This model is based on the “Abstracted Common Model” developed by the CMU CERT technical staff and additionally included the factors of social networks, insider motivations, and organizational priorities. The Abstracted Common Model was selected as it was deemed most relevant and understandable for the audience of USAF leaders and supervisors.

Based on the findings of the policy review, this research offers actionable recommendations that the USAF could implement in order to better prevent, detect, and respond to malicious insider attacks. In addition, this research proposes three new best practices that can be used by any organization to mitigate this threat to security.

1.3 Scope

In the article "Analysis of End User Security Behaviors," Stanton et al. (2005) describe security incidents in terms of the intention (malicious, neutral, or beneficial) and expertise (high or low). While incidents of a neutral or beneficial nature may actually do harm to an organization, such as "dangerous tinkering" and "naïve mistakes" (Stanton et al., 2005), this research focuses on incidents of a malicious nature. Though malicious acts requiring high expertise, termed "intentional destruction," are often the most dangerous, those requiring low expertise ("detrimental misuse") are included as well (Stanton et al., 2005). These acts of detrimental misuse may be precursory actions and should not be ignored.

In risk assessment, a threat-source is an entity that exploits a vulnerability (Elky, 2006). While threats can come from many different sources, to include weather or an electrical disruption, this research is only concerned with situations where malicious insiders (i.e., people) are the threat-sources.

This research focuses on two categories of insider threat, sabotage and espionage, which are deemed most relevant to the USAF. Sabotage is the destruction of company resources, such as deploying a logic bomb, while espionage entails the stealing and selling of company information.

The intended audience of this research includes USAF leaders, supervisors, and network professionals, especially those with the authority to affect and implement organizational policies, controls, and climate. The research is purposefully written to make the subject matter understandable to those without a technical background in information technology or any of the modeling types. The problem of insider threat is one which is mitigated only through a group endeavor, from high-level organizational leaders to the front-line supervisors; in fact, the immediate supervisor is perhaps the strongest part of the overall defense against insider threats.

1.4 Thesis Organization

This chapter described the significant problem that malicious insider attacks pose on today's organizations and briefly explained the objectives of this research. Chapter II presents the current information published on insider threat, to include the variables that come into play and historical case studies. Existing insider threat models are discussed, as well as background information regarding logical data and systems dynamics modeling. Chapter III explains this research's process for modeling the problem, including the initial development of a logical data model and a system dynamics model. This chapter also discusses the selection of the Abstracted Common Model as the basis of this research's Insider Threat Model for Sabotage and Espionage, which is used in the USAF policy review. An explanation is also given of the incorporation of motivations, organizational priorities, and social networks into this research's final model. Chapter IV explains the methodology for the review of the DoD and USAF policies in terms of insider threat mitigation measures, to include the best practices published by the CMU CERT technical staff. The results of the policy review are presented, as well as recommendations aimed to assist the USAF in battling the insider problem. In addition, this research proposes three new best practices that can be implemented by any organization. Finally, Chapter V provides a summary of the research along with a discussion of its conclusions and impact. Recommendations for future research are also provided.

II. Literature Review

2.1 Overview

There is no definitive profile for a malicious insider or for an organization that will suffer an insider attack. From analyzing case studies of actual attacks, researchers have found themes and commonalities. This chapter discusses the current information published on insider threat, in particular the various factors and their incorporation into existing models. Two historical case studies are presented in detail to further demonstrate how these factors come into play. This chapter also provides background information on logical data modeling and system dynamics modeling as both are used in the models developed in this research.

2.2 Factors in the Insider Threat Problem

In examining the insider threat problem, current research articles and models focus on one or more of the following factors: insider precursors, expectations, and motivations; organizational controls, priorities, and trust; social networks; and event triggers. This next section defines and takes a closer look at each of these.

2.2.1 Precursors of the Malicious Party

From analyzing case studies of famous insider attacks, researchers have found that the orchestrators shared psychological, professional, legal, and economic characteristics and behaviors, as well as committed similar technical precursory incidents leading up to the actual attacks.

Historically, malicious insiders have been described as intelligent, dishonest, egotistical, passionate, and instable (Tuglular, 2000). In addition, malicious insiders often lack strength of character and self-control and are prone to taking risks. They frequently have poor social skills (Tuglular, 2000) and are resistant to change (Cappelli et al., 2007). Malicious insiders may also have participated in unusual sexual behavior and had addictions to alcohol, drugs, or gambling (Under Secretary for Management, 2006). Before launching attacks, insiders have often exhibited certain behaviors, such as making alarming statements and acting out of character (Puleo, 2006).

In terms of the malicious parties' professional life, they often exhibited poor, declining, or inconsistent job performance; examples include failing to meet deadlines, inability to handle an appropriate workload, and absenteeism. In addition, they may have been dissatisfied with their job and believed they had poor job security (Puleo, 2006). Although not all insider attacks require a lot of skill, the case studies show that the malicious parties often possessed strong professional skills, such as those in the realm of information technology. In addition, they usually had acquired a substantial amount of professional knowledge regarding their organization's structure, information systems, and security policies and controls (Tuglular, 2000).

A similar problem to trying to identify traits and behaviors of malicious insiders is that of trying to decide who in an organization can be trusted with classified information. Again, there is no exclusive set of factors, but the federal government has created the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" (Under Secretary for Management, 2006). One of the areas of focus for these guidelines is whether individuals have a criminal record. If they do, they may be predisposed to illegal or immoral activity. Another area examines the individuals' financial situation, to include economic stability and security, as well as the presence of any unusual activity. If employees are having, or have had, legal or financial problems, they may be susceptible to blackmail or solicitations to commit espionage (Under Secretary for Management, 2006).

Technical precursors are common in insider threat cases. In terms of sabotage attacks, insiders usually preferred to "test the waters" before launching the full-blown attack. In addition, certain activities may have needed to take place in order for the attack to be successful and possibly even more devastating, such as the destruction of recovery materials. In espionage attacks, insiders have often conducted unusual or unauthorized behavior on the network in order to obtain the information they needed. Examples of precursory incidents include the following: accessing unauthorized websites, installing unauthorized software, cracking passwords, escalating one's privileges, creating covert channels, sending coded messages (Mills et al., 2009), social engineering, orchestrating a denial of service attack, purposefully not completing their job-related duties, masquerading, unauthorized reading or modifying of resources (Phyo and Furnell, 2004), stealing or hiding data, spamming, downgrading classifications, modifying activity logs, and redirecting output (Brackney and Anderson, 2004).

Figure 1 shows a taxonomy of observable precursors that was developed at a Advanced Research and Development Activity (ARDA) workshop. This single figure combines many of the factors discussed earlier, to include technical precursors, economic situation, and addictions. This taxonomy reiterates the broad range of behaviors that can possibly come into play in the complex insider threat problem.

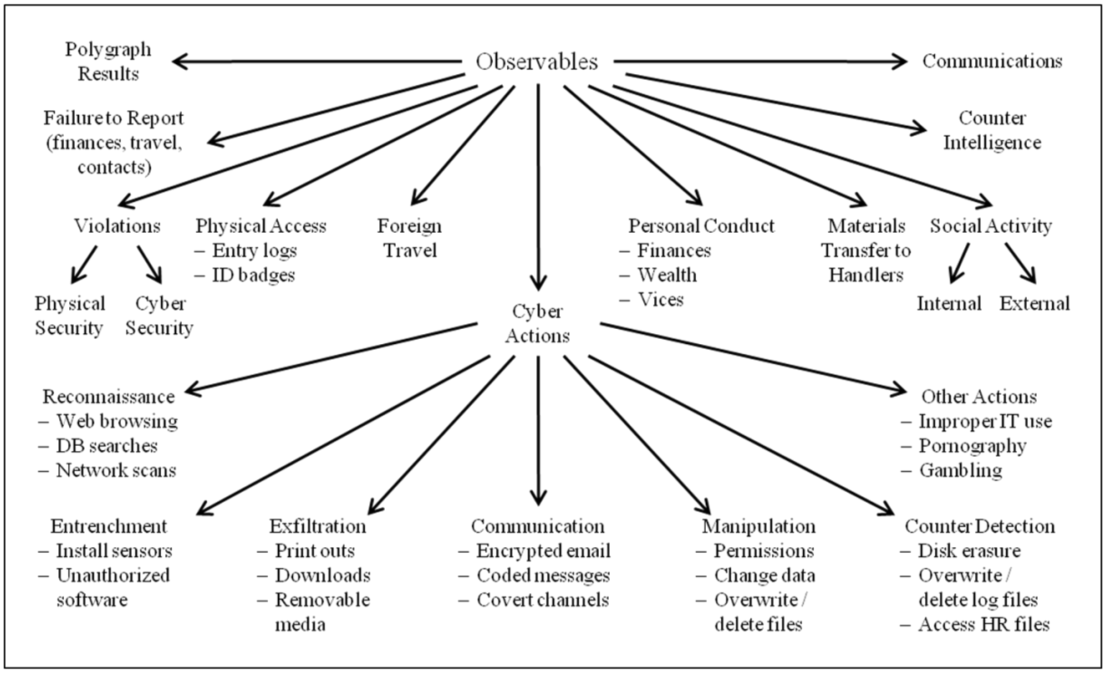

Observables
Polygraph Results
Communications
Failure to Report (finances, travel, contacts)
Counter Intelligence
Violations
Physical Access – Entry logs – ID badges
Foreign Travel
Personal Conduct – Finances – Wealth – Vices
Materials Transfer to Handlers
Social Activity
Physical Security
Cyber Security
Cyber Actions
Internal
External
Reconnaissance – Web browsing – DB searches – Network scans
Other Actions – Improper IT use – Pornography – Gambling
Entrenchment – Install sensors – Unauthorized software
Exfiltration – Print outs – Downloads – Removable media
Communication – Encrypted email – Coded messages – Covert channels
Manipulation – Permissions – Change data – Overwrite / delete files
Counter Detection – Disk erasure – Overwrite / delete log files – Access HR files

Figure 1. Cyber Event/Observable Taxonomy (Mills et al., 2009)

2.2.2 Insider's Expectations

The recognition, rewards, freedoms, and responsibilities that insiders expect from their management can also play a role in whether they commit malicious acts. In all manager-employee relationships, there are psychological contracts, or unwritten agreements, between the two parties (Robbins and Judge, 2008). If managers do not fulfill employees' expectations, the employees may become disgruntled (Moore et al., 2008). As mentioned earlier, a common trait of malicious insiders is egotism. Many feel they deserve frequent recognition, in terms of raises, promotions, and additional authority or responsibility. If they feel they are underappreciated, they may decide to commit espionage to earn more money or to commit sabotage as retaliation against the company.

2.2.3 Event Triggers

Certain events can be factors in the insider threat problem. Most commonly, events can increase or decrease an insiders' motivation to launch an attack. Negative events may worsen the mental, economic, or professional state of insiders, and they may become more enticed to seek retaliation or profit. On the other hand, positive events may lessen their motivation as they may not want to risk their improved status. An event may be at the individual level, such as a marriage, divorce, birth of child, death in family, or health issue (Puleo, 2006). A negative event (from the insider's perspective), such as an assignment to a more demanding supervisor, can lead to a decrease in expectation fulfillment and in turn increased disgruntlement (Moore et al., 2008). Events may also be at the organizational level, to include restructuring, mergers, personnel cuts, and relocation.

Recent articles have shown that nationwide events, such as the current economic situation, can also trigger malicious insider activity. In uncertain times employees can become nervous about layoffs or disgruntled over not receiving a bonus or promotion. In 2008 a disgruntled employee of the city of San Francisco intentionally altered administrative passwords, locking out the rest of the company from critical network resources for days (Vijayan, 2008). This year it was discovered that a former Fannie Mae contractor had planted malicious software on the company's network after being terminated (McMillan, 2009).

2.2.4 Social Networks

The relationships that insiders have within an organization can play into the insider threat problem in two different and opposing ways. Per the Social Bond Theory, insiders who have strong relationships with their managers or co-workers are less likely to commit a malicious act. If insiders feel attached to their co-workers, they do not want to lose these friendships either by their co-workers' disapproving of their actions or the company firing them (Theoharidou et al., 2005). In a study looking for possible predictors of withdrawal behaviors, a strong negative correlation was found between co-worker satisfaction and unexcused absenteeism. The author theorized that this was due to the employees not wanting to risk the friendships they had made with co-workers by exhibiting deviant behavior (Blau, 1985). Additionally, insiders may feel committed to these co-workers and not want to bring harm to them professionally by executing an attack on the organization's assets (Theoharidou et al., 2005). Historical attacks have resulted in loss of customers and contracts, destruction of an organization's critical information and assets, decrease in worker productivity, and damages equaling millions of dollars (Melara et al., 2003).

Workplace relationships could also increase insiders' motivation to commit a malicious act. Per the Social Learning Theory (Theoharidou et al., 2005), employees who associate with co-workers who are breaking the security policies may be more inclined to commit wrongful acts, whether it is in conjunction with these role models or by themselves (Theoharidou et al., 2005). The insiders may rationalize that the deviant behavior is acceptable, especially if the co-workers are receiving benefits from it or, at the very least, not getting caught.

2.2.5 Insider Motivations

As mentioned in the first chapter this research focuses on those insiders with malicious intentions. While many factors, such as psychological traits, relationships, and event triggers, can increase or decrease their motivation to attack, according to Casey (2004) the source of the motivation is one or more of the following:

- *Power reassurance (compensatory)*: mildly aggressive acts committed to see if the attacker has the ability to accomplish them, boosts self-confidence (Mills et al., 2009)
- *Power assertive (entitlement)*: moderately to highly aggressive acts used to boost self-worth at the expense of the victims. Attackers want to show the victims they are more skilled than and have authority over the victims (Casey, 2004).
- *Anger retaliatory*: highly aggressive acts, to include sabotage, used to gain revenge; one of the two most common motives (Mills et al., 2009)
- *Anger excitation (sadistic)*: highly aggressive, personal act used to gain pleasure (Mills et al., 2009)
- *Opportunistic*: mildly aggressive acts used to achieve satisfaction, often viewed as having a small chance of being detected (Mills et al., 2009). This motivation type aligns with the General Deterrence Theory which states that people base their decisions on maximizing benefit while minimizing cost (Theoharidou et al., 2005).
- *Profit oriented*: varying in aggressiveness, often coupled with greed (Shaw et al., 1998) and power reassurance, includes espionage; other most common motive (Mills et al., 2009)

2.2.6 Organizational Controls

Organizational controls are put into place to help protect an organization from attacks, from both insiders and outsiders. Ideally these controls deter or prevent an attack, but at the very least detect if one has occurred. Organizational controls can be grouped into one of the following three categories: technical, formal, and informal (Melara et al., 2003). Ideally, an organization implements measures from all three groups.

- *Technical*: includes technical monitoring (to include network traffic, e-mail traffic, and file access), auditing and disabling access paths (Cappelli et al., 2007), recovery software, antivirus software, backups (Melara et al., 2003), identification and authentication procedures, cryptography, discretionary access control, (Stoneburner et al., 2002)
- *Formal*: includes employee intervention, sanctions (such as demotion, termination, and decrease in authority or privilege levels), termination threshold and time policies (Cappelli et al., 2007), segregation of security duties, existence of a separate security department, risk evaluations, policies regarding authority and privilege levels (Melara et al., 2003)
- *Informal*: culture, values, education and training (Melara et al., 2003), warnings about repercussions (Rich et al., 2005)

It is important to note that controls, such as sanctions, may have the opposite effect of what is intended. If disgruntled employees are reprimanded for unauthorized activity, they may become even more disgruntled and increasingly likely to commit an attack. In such a case, it may be wise to supplement the issuing of sanctions with employee intervention (Cappelli et al., 2007).

للاستشارات المنارة

2.2.7 Organizational Priorities

The priorities of an organization help to form its attitude regarding security. An organization that highly values profits may not find it financially advantageous to invest a lot of time and money into security controls. On the other hand, a company who highly values its reputation and feels it cannot risk a high-profile security incident may spend more money on security measures (Rich, et al., 2005). Furthermore, if an organization views a certain system as especially vital, it is usually willing to invest more into controls to protect that system (Mills et al., 2009). In most cases, insiders are privy to the company's stance on security and know whether or not it wise to attempt an attack.

2.2.8 Organizational Trust

As mentioned earlier, one of the most difficult aspects of the insider threat problem is that the insider is trusted by the organization. Trust is an element of any relationship, including those between employees and their managers. Most research breaks down trust into components; this research uses those outlined in the research by Mayer et al. (1995). Put into the context of a work relationship, they are as follows:

- *Ability*: one's skill set and competency in the domain of the task at hand
- *Benevolence*: one's desire to execute the task well for his manager and the organization
- *Integrity*: one's set of morals or values and how they align with the manager's

Initially managers are basing their trust in a new employee on calculative trust, which includes factors such as the employee's reputation, education, certifications, and resume (Rousseau et al., 1998). At all times, institutional-based trust plays a role; this type of trust includes the organization's controls and mechanisms. For example, initially managers trust the new employee since they believe the company's interviewing and clearance processes are sound. Managers have confidence that the company selected a qualified person, one who is capable to do the job, has the best interest of the company in mind, and is moral. Throughout the relationship, most managers continue to use clearance renewals, as well as company policies, procedures, and controls, to assist in reevaluating the employee's trustworthiness (McKnight et al., 1998). The managers also base their trust on their own experiences with and judgments of the employee, known as relational trust (Rousseau et al., 1998). The type of business an organization conducts most likely affects how initially trusting it is of its employees. Again, this is usually discernable by the insiders, as they see how freely authority and privileges are given out.

Trust can be a tricky element within an organization, especially in terms of security. If an organization is very trusting of its employees, it may not invest as much into security controls. The lack of controls, such as employee on-line monitoring, could reduce the probability of preventing or detecting malicious insider activities. With little or no reported incidents, the company may cut back even more on security measures. Sadly, while incidents may not be detected or reported, they could be occurring just the same; companies need to be mindful of this "trust trap" (Moore et al., 2008).

2.2.9 Risk Management

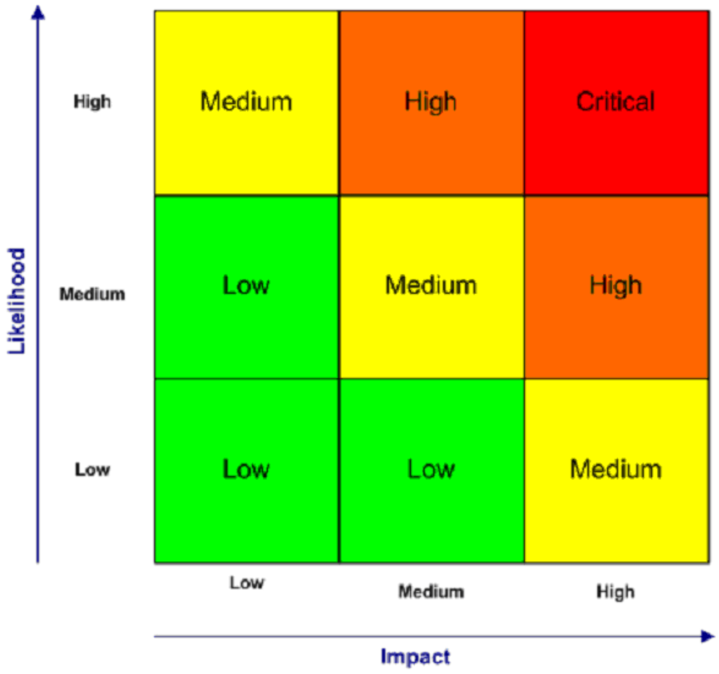
The insider threat problem is inherently built on the concept of risk management. An organization must balance the costs and benefits that are inherent with cyber security. The most obvious cost is money for the information security personnel and resources. In an environment in which every employee and network activity could be completely monitored and analyzed, it might be possible to prevent all attacks. Of course, no organization has the time, money, or personnel to create and maintain such an environment. Often companies worry most about undetected threats, also called false negatives, but there is a danger and cost to false positives, or false alarms, as well (Martinez-Moyano et al., 2008). They can result in employees being sanctioned for non-malicious acts or resources being wastefully used to investigate benign events.

In any discussion of risk management there are the following basic elements:

- *Threat-source*: entity which intentionally or accidentally triggers a vulnerability. As stated earlier, this research is only concerned with malicious insiders as the source of threats (Elky, 2006).
- *Threat*: potential of threat-source to trigger or exploit vulnerability. Examples of threats include information disclosure, alteration of software, inappropriate bandwidth usage, denial of service, alteration of data, configuration error, and telecommunication interruption or malfunction (Elky, 2006).
- *Vulnerability*: flaw or weakness in a system within the organization that can be triggered or exploited. This flaw could be in the design or implementation of the system, or in the security procedures and controls meant to protect it. Examples of vulnerabilities include unpatched systems, weak firewall settings, and policies that do not require the timely termination of employees' physical access to company facilities (Stoneburner et al., 2002).
- *Likelihood*: probability that a threat will be successfully exercised against a vulnerability. Often this is measured qualitatively as low, moderate, or high (Elky, 2006).

- *Impact*: combination of losses in terms of confidentiality, integrity, availability, as well as effects on mission capability, assets, and human life. This often measured qualitatively as low, moderate, or high (Elky, 2006).
- *Risk*: determined by analyzing the predicted likelihood and impact of the threat to the vulnerability. Again, this is often measured qualitatively as low, medium, high, or critical (Figure 2).

The risk management process assists organizations in deciding which threat-vulnerability pairs to address first. Obviously those of high or critical risk are the ones on which managers should focus. To reduce the risk to a system, an organization must first



Likelihood	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Figure 2. Example Risk Level Matrix (Mills et al., 2009)

become more aware of its current state, to include its information resources; those resources' vulnerabilities; the motivations, skills, knowledge, and resources of its employees; and the controls it has in place to attempt to prevent attacks. It can estimate the likelihood of different threat-vulnerability combinations and determine the resulting impact (Stoneburner et al., 2002). An organization is then prepared to work towards lessening the likelihood, impact, or both. Additional or improved organizational controls can help to decrease vulnerabilities as well as the impact, such as maintaining back-up or redundant systems.

2.3 Case Studies

To illustrate how these many individual and organizational factors play into the insider threat problem, two of the most famous attacks, committed by Robert Hanssen and Timothy Lloyd, are presented below.

Robert Hanssen was an FBI agent who possessed a Top Secret/Sensitive Compartmented Information clearance and committed espionage for over 15 years. During this time, he sold thousands of pages of classified documents to agents of the Union of Soviet Socialist Republics (USSR), and later Russia, to include information on the United States' nuclear defense strategy (PERSEREC, 2004) and counterintelligence tactics (Herbig and Wiskoff, 2002). Hanssen also shared information about the existence of a tunnel underneath the Russian embassy which the U.S. used to spy on them (Herbig and Wiskoff, 2002). He also identified three Russian spies who were working for the FBI, two of whom were later executed (PERSEREC, 2004). Hanssen committed this espionage by breaking into classified computer files which he had no need to access for his legitimate FBI responsibilities. He also used his knowledge of information systems to access FBI case files in order to monitor any possible investigations the FBI was conducting on him (PERSEREC, 2004). In addition to the loss in human lives, Hanssen's actions resulted in significant damage to the national security of the United States.

During his time with the FBI, Robert Hanssen could be described as intelligent, dishonest, and egotistical, as well as a risk-taker. A former co-worker said that despite his intellect, he did not possess strong social skills and was an introvert (Cooper and Garvey, 2001). Given the number of years he worked in the FBI, he had ample time to learn its inner workings. He was also skilled in the realm of information technology and computer security. Through his various jobs within the FBI, Hanssen gained access to many FBI case and counterintelligence databases, to include ones owned by the NSA, CIA, and the State Department (Herbig and Wiskoff, 2002).

Robert Hanssen lived well above his means as a federal employee. He paid for the down payment and remodeling on his Washington D.C. home in cash, and he sent his six children to expensive private schools (Havill, 2001b). Despite the supplementary income from his espionage, Hanssen managed to accumulate a significant amount of debt, totaling more than $275,000 at one point in time (PERSEREC, 2004). Hanssen also had an extramarital affair with a stripper, on whom he allegedly spent a sizeable portion of the money he made from his work with the Russians (PERSEREC, 2004). Robert Hanssen was clearly motivated by profit and greed. It has also been speculated that he was disgruntled with the FBI, perhaps enticing him to retaliate against the organization (PERSEREC, 2004). Given his egotistical nature, he most likely enjoyed the thrill of being able to commit his illegal acts, especially while working for such a prestigious organization as the FBI.

Timothy Lloyd worked for the Omega Engineering Corporation for 11 years, making his way up to the position of system administrator. He was subsequently demoted and fired from the company, but before he left, he loaded a software "time bomb" onto the network that was programmed to deploy once he was gone (Melara et al., 2003). Lloyd worsened the effects by stealing backup tapes and changing a company policy to centralize the storage of company programs, replacing the former method of housing them on numerous workstations. The destruction from the bomb cost the company more than $10 million in damages to hardware and software, decreased productivity, and lost customer revenue (Melara et al., 2003).

Like Hanssen, Lloyd was intelligent, unscrupulous, and egotistical, as well as instable towards the end of his time with Omega. Lloyd's expectations were rarely met, and he seldom felt he received the recognition he deserved. He was extremely unhappy when Omega Engineering Corporation expanded and his authority became diluted. After being demoted, Lloyd began to physically and verbally abuse his co-workers and to purposefully slow down projects (Melara et al., 2003).

Lloyd had extensive knowledge of the company's policies, structure, and information systems. He developed much of the network on which Omega depended and was well aware of its weaknesses and vulnerabilities. As system administrator, he created many of the company's security policies (Melara et al., 2003). Before launching the software "time bomb", he caused a number of smaller network incidents aimed at decreasing performance and causing downtime on the network. He was most likely motivated by his need for revenge and increased self-worth.

2.4 Insider Threat Models

To better understand the variables that can come into play in the insider threat problem and how they affect each other, previous insider threat research has modeled this problem. This section presents eight models published in previous insider threat research. These models focus on one or more of the factors discussed earlier in the chapter. This section also gives a brief description of logical data and system dynamics modeling, to include the symbols used and example models. These two types of modeling were used in this and previous research.

2.4.1 Voltaire

Laird and Rickard (2005) proposed a system called Voltaire that could be used to help mitigate insider threat issues by detecting unusual computer use behavior that could be technical precursors. The first step in the system is to develop a model of "normal" behavior for each user in a given organization, looking at document access, network usage, and semantic content of documents. Once these profiles are established, the insiders are monitored for unusual behavior. The system also looks for inappropriate behaviors that were present in past insider threat cases. Examples of the dimensions that the system analyzes are below:

- Documents Deleted From Database
- Documents Modified versus Read Ratio
- Documents Read versus Written Ratio

- Documents Printed
- Printing Other Users' Documents
- Different Printers Used
- Number of Databases Accessed
- Specific Databases Accessed
- Latest Work End Time
- Earliest Work Start Time

2.4.2 Risk Predictor Model

Puleo (2006) developed the "Risk Predictor Model" that examines human behaviors and outside influences to determine insiders who have a higher potential of committing a malicious act. The model is comprised of the following four components:

- *Influence Matrix*: how different influences (such as stress, pay cut, relationship with family, and family financial status) affect one another
- *Event Matrix*: how events (such as financial loss, change in physical health, and recent termination) affect influences
- *Response Vector*: how strongly insiders are affected by each influence (For example, individuals may have a lot of stress, but solid relationships with their families help them to handle it well.)
- *Stimulus Vector*: if an event has occurred in an individual's life

Versions of these matrices and vectors are created to represent a typical employee. These standards can then be used to compare to actual insiders and detect those who deviate significantly from the average.

2.4.3 Multidiscipline Approach to Mitigating the Insider Threat

The "Multidiscipline Approach to Mitigating the Insider Threat" (MAMIT) model (see Figure 3) combines numerous factors discussed earlier. It examines the motivations of the insiders, to include opportunity, as well as observes their behaviors, actions, and network usage. This model also incorporates elements of risk management, to include threats and vulnerabilities. The Centralized Analyst or Agent compiles indicators and produces individual and organizational threat levels. The individuals with threat levels that are greater than the acceptable organization threat level are tagged as potential

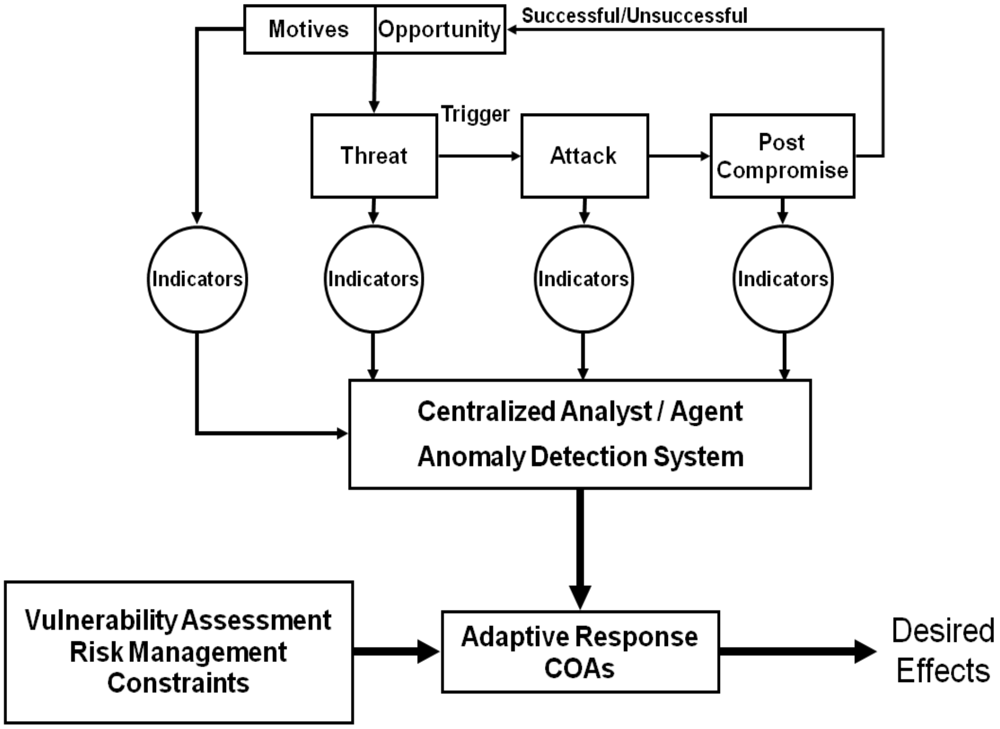

Motives
Opportunity
Successful/Unsuccessful
Trigger
Threat
Attack
Post Compromise
Indicators
Indicators
Indicators
Indicators
Centralized Analyst / Agent
Anomaly Detection System
Vulnerability Assessment
Risk Management
Constraints
Adaptive Response
COAs
Desired Effects

Figure 3. MAMIT (Butts, 2006)

malicious parties. Upon identifying a potential threat-source, possible courses of action are to warn management, increase monitoring of the tagged insider, and lock-out the insider from network systems. Some actions could be made automatically and based solely on network activity, while others may necessitate the existence of past behaviors or job-related incidents and require managerial approval (Butts, 2006).

2.4.4 Logical Data Modeling

Before presenting Tuglular's (2000) structural approach to insider threat, which is the inspiration for this research's first model, "Insider Threat Logical Data Model," this section provides background information on logical data modeling.

2.4.4.1 Background Information on Logical Data Modeling

Logical data modeling, also called entity-relationship (E-R) diagramming, provides a way to study entities of interest, specific attributes of interest, and the relationships between entities (Department of Defense, 2007). For a business organization, example entities include personnel, resources, policies, and products. Attributes are used to describe the entities in more detail, such as a person's name, position within the company, and security clearance. Relationships are then determined to depict the associations between entities, such as manager/subordinate and peer/peer relationships and job functions. The purpose of logical data modeling is to better understand the resources of an organization, to include what information about them is important and how they interact with each other. This type of modeling is often done when designing databases to ensure all the correct information and tables are included and developed. Figure 4 depicts a very simple logical data model for a real estate

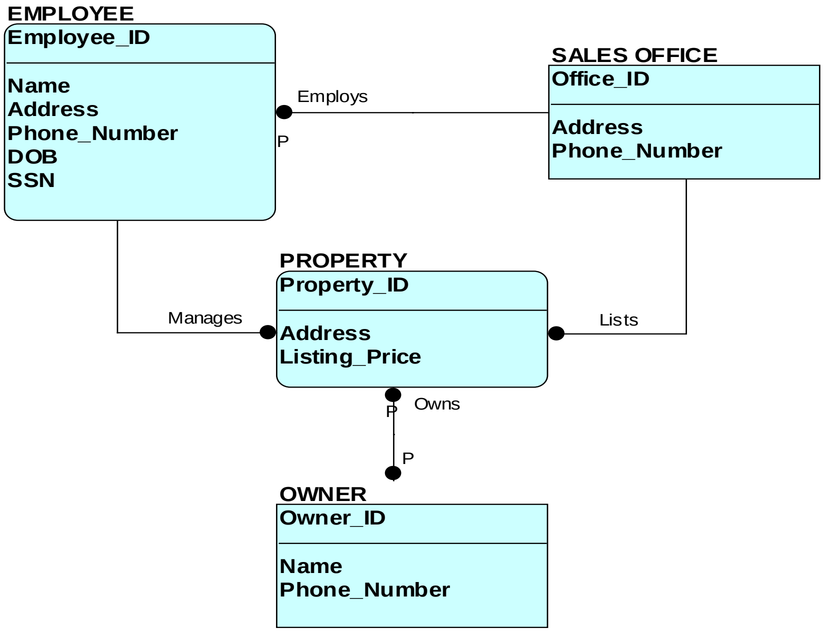

EMPLOYEE
Employee_ID
Name
Address
Phone_Number
DOB
SSN
Employs
P
SALES OFFICE
Office_ID
Address
Phone_Number
PROPERTY
Property_ID
Address
Listing_Price
Manages
Lists
Owns
P
P
OWNER
Owner_ID
Name
Phone_Number

Figure 4. Logical Data Model Example

company. The level of detail required depends on the nature of the problem being solved.

Figure 4 shows four different entities: *EMPLOYEE*, *SALES OFFICE*, *PROPERTY*, and *OWNER*. Each entity is a noun—person, place or thing—and has various attributes used to describe that entity. For example, an *EMPLOYEE* has an *Employee_ID*, as well as a *Name*, *Address*, *Phone_Number*, *DOB*, and *SSN*. Usually, there is a primary key that uniquely identifies a specific member of that entity class, such as *Employee_ID*. The model also shows the relationships between the entities. Relationships are represented with verb or verb phrase names to show how one entity interacts with or depends on another. For example, a *SALES OFFICE* "Employs" an *EMPLOYEE*. Various types of relationships exist, but the ones that are of most interest here are *identifying* and *non-specific* relationships. An identifying relationship is also referred to as a parent-child relationship. In a parent-child relationship, the child entity cannot exist without the parent, and the parent's primary key(s) (PK) migrates to the child entity as a foreign key (FK). A single parent may have multiple children, but a child can have only one parent.

A non-specific relationship is one in which "an instance of either entity can be related to a number of instances of the other entity" (Colombi, 2008). Relationships can also have cardinality, which identifies how many of each entity there may be. Figure 5 presents the symbols for the types of relationships and cardinality used in this research's model.

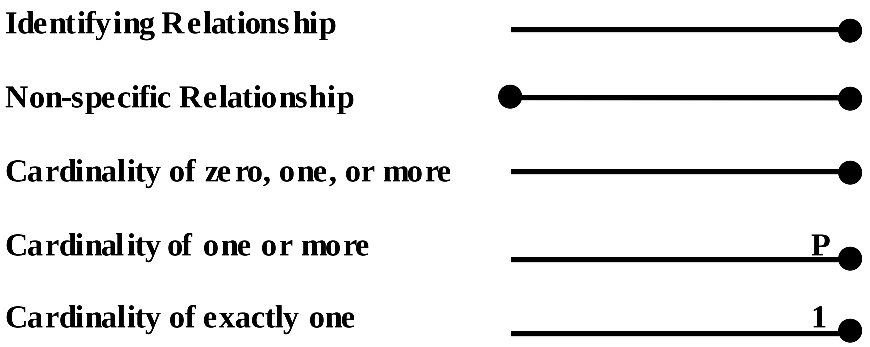

Identifying Relationship
Non-specific Relationship
Cardinality of zero, one, or more
Cardinality of one or more
P
Cardinality of exactly one
1

Figure 5. Logical Data Model Symbols (Colombi, 2008)

2.4.4.2 Structural Approach to Insider Computer Misuse Incidents

Tuglular's (2000) structural approach to the insider threat problem focuses on the following three main entities, which all have many subcomponents:

- *Incident*: target (threat realized, value, and control), subject (reason), method, place, time
- *Response*: recognition, trace information, evidence, suspect (profiles, qualifications, and access authorization)

- *Consequences*: disruption (confidentiality, integrity, and availability), loss (financial, morale, clients, publicity, and productivity), effect, violation (policies), result

Tuglular viewed these entities as the foundation from which future insider threat detection systems could be created. This approach aims to identify potential malicious insiders by continuous and extensive information collection. By analyzing incidents to a greater level of detail, he hoped to better prevent future attacks.

2.4.5 System Dynamics Modeling

Before presenting the remaining five insider threat models, this section provides background information on system dynamics modeling as it used in all of them. The final model, "Model of the Insider IT Sabotage Problem," was the basis for this research's second model, entitled "Insider Threat System Dynamics Model."

2.4.5.1 Background Information on System Dynamics Modeling

System dynamics modeling can aid in better understanding a complex problem by diagramming its variables and how they affect each other over time (Moore et al., 2008). In the example depicted in Figure 6, the variables include *overtime hours required* and *work done*. Furthermore, arrows represent the relationships between variables, and each relationship has a source and target. In Figure 6, *overtime hours required* is the source of two relationship arrows and the target of one. These relationships show the influence that two variables might have on each other. Relationships show either positive or negative correlation. For the example in Figure 6, there is a negative correlation between *fatigue* and *quality of work*; as *fatigue* increases, *quality of work* decreases. Symbology used to represent these relationships varies. In Figure 6, a positive correlation is shown using a

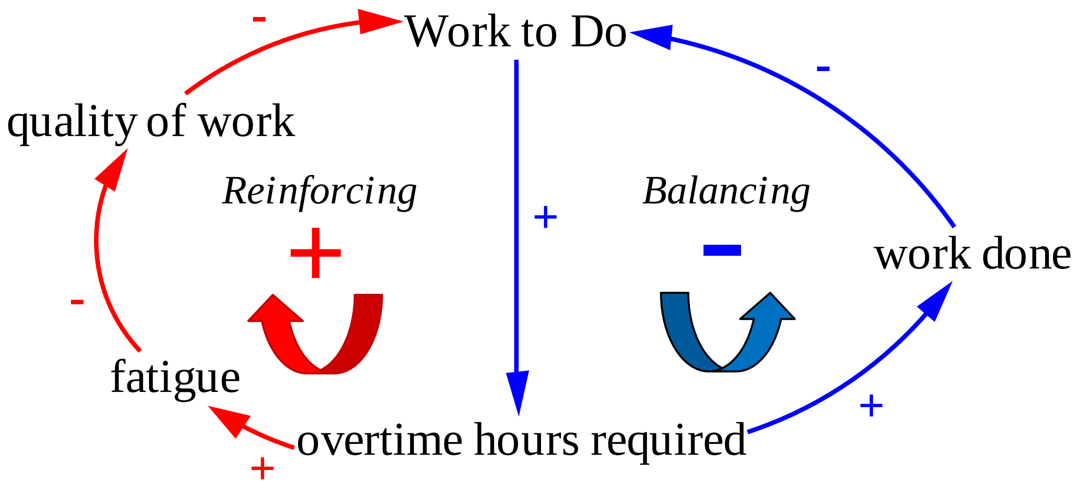


Figure 6. System Dynamics Modeling Example (Ventana Systems, Inc., 2007)

'+' sign, and a negative correlation is indicated by a '-' sign. A positive correlation can also be depicted by a solid line or letter 'S' (for "same"), while a negative correlation can be indicated by a dashed line, or 'O'(for "opposite").

Complex system dynamics models often include feedback loops that are either *balancing* or *reinforcing;* some references refer to these as *negative* and *positive*, respectively (Sterman, 2000). A balancing loop models a situation where the relationships between two or more variables lead to a goal state. Though change is occurring, the variables are working to establish and maintain an equilibrium condition. A reinforcing loop is essentially the opposite; the relationships between these variables are continuously driving the values either upward or downward (Moore et al., 2008). In Figure 6, the red, positive loop is reinforcing as *Work to Do* is continually increasing. As the amount of work to do increases, employees are required to work more overtime hours. If the overtime causes fatigue, the quality of work will actually decrease. This initiates a vicious cycle because work will have to be reaccomplished, which in turn could lead to even more overtime hours. On the other hand, if the employees do not experience fatigue and are successfully able to accomplish high quality work during the overtime hours, they will have less work to do. This second scenario is a balancing loop and is depicted by the blue, negative loop in Figure 6.

Sometimes "stock and flow" symbols are used in system dynamics modeling to represent the levels and rates of variables in a problem. A *stock* represents a level of a variable in the problem, and it can have both an *inflow* and an *outflow*. The *inflow* comes from a *source* and *outflow* goes into a *sink*. Figure 7 illustrates these stock and flow components.

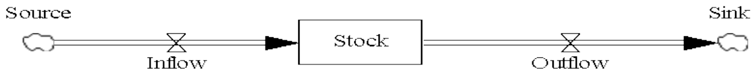

Source
Inflow
Stock
Outflow
Sink

Figure 7. Stock and Flow Symbols (Ventana Systems, Inc., 2007)

Figure 8 illustrates a simple example which models rabbit population, taking into consideration factors such as birth rate and life expectancy.

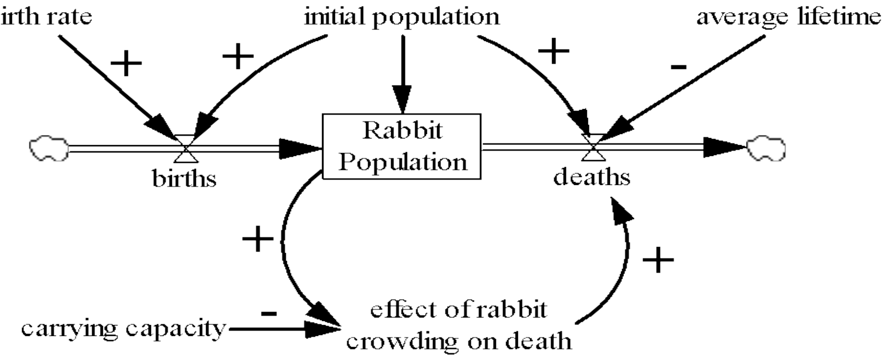

birth rate
initial population
average lifetime
+
+
+
-
Rabbit Population
births
deaths
+
+
-
carrying capacity
effect of rabbit crowding on death

Figure 8. Stock and Flow Example (Ventana Systems, Inc., 2007)

2.4.5.2 Insider Attack on an Information System

One method for analyzing the insider threat problem is to model one specific case study. In the "System Dynamic of Insider Attack on an Information System" (see Figure 9) developed by Melara, et al. (2003), the authors analyzed the case study of Timothy Lloyd's attack at the Omega Engineering Corporation. Melara, et al. (2003) focused on Lloyd's precursory incidents and aggressive acts, which they felt both stemmed from his discontent and disgruntlement with the company. Since Lloyd's technical precursors were primarily causing downtime on the information systems, *downtime* was a primary variable, analyzed in terms of impact and recovery. The model also looked at Omega Engineering's commitment to security (or lack thereof), its formal controls, and its decision to fire Lloyd.

Once created and validated, the model was tested by analyzing how variables such as *management perception of technical security*, *technical security reduction*, and *technical security level* are affected over time by varying levels of formal controls (ranging from "no" to "high"). In all three cases the implementation of high formal controls resulted in positive effects for the organization, to include increased management perception of technical security, decreased reduction in security by insider, and increased technical security level (Melara et al., 2003).

2.4.5.3 Insider IT Sabotage Model

The CMU CERT technical staff has developed many system dynamics models, including the "Insider IT Sabotage Model" (see Figure 10) (Band et al., 2006). This model contains attributes of the insider, to include disgruntlement, predispositions, stress,

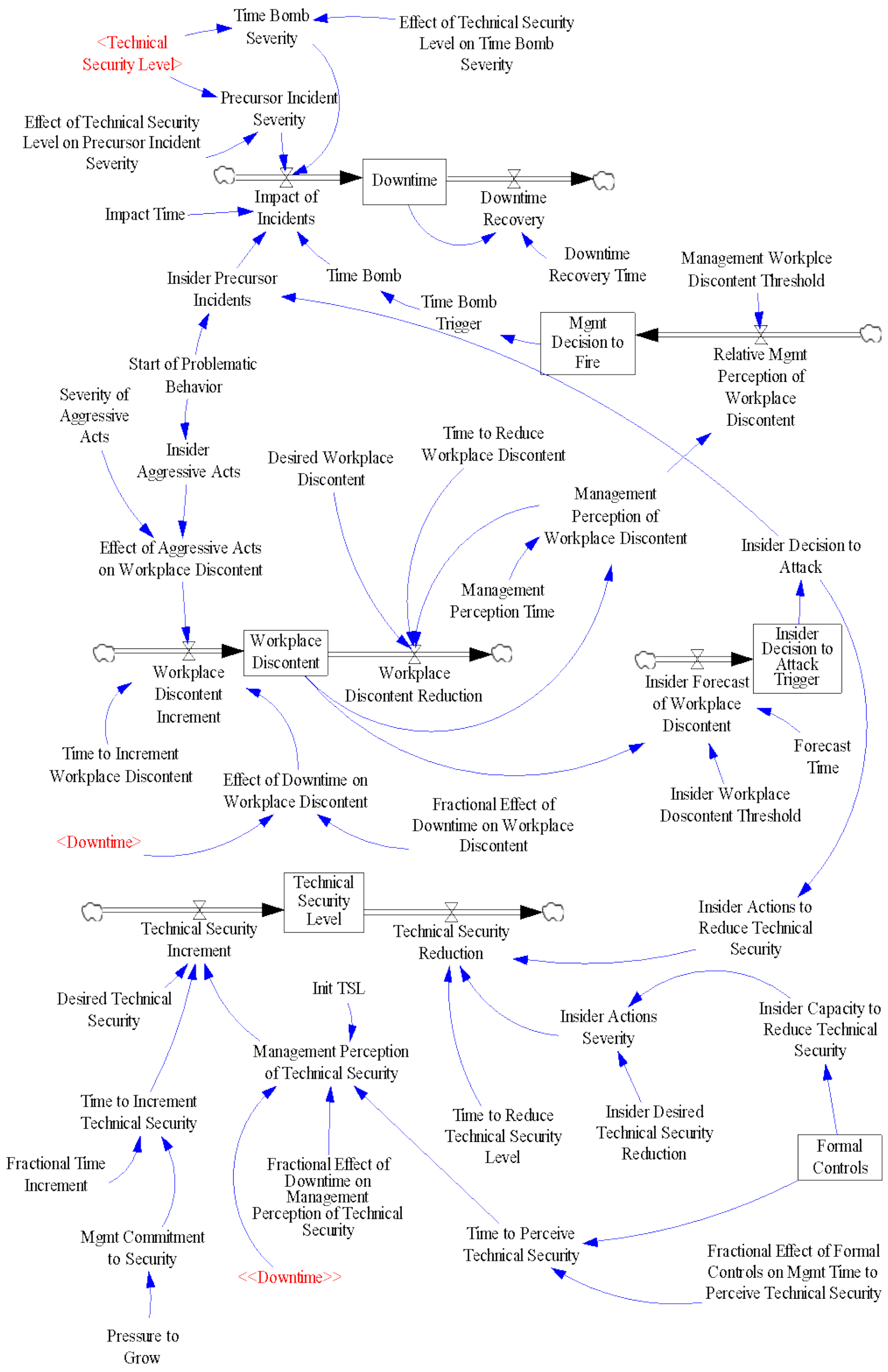

Time Bomb Severity
Effect of Technical Security Level on Time Bomb Severity
<Technical Security Level>
Precursor Incident Severity
Effect of Technical Security Level on Precursor Incident Severity
Downtime
Impact of Incidents
Downtime Recovery
Impact Time
Downtime Recovery Time
Management Workplce Discontent Threshold
Insider Precursor Incidents
Time Bomb
Time Bomb Trigger
Mgmt Decision to Fire
Relative Mgmt Perception of Workplace Discontent
Start of Problematic Behavior
Severity of Aggressive Acts
Insider Aggressive Acts
Desired Workplace Discontent
Time to Reduce Workplace Discontent
Management Perception of Workplace Discontent
Insider Decision to Attack
Effect of Aggressive Acts on Workplace Discontent
Management Perception Time
Workplace Discontent
Workplace Discontent Increment
Workplace Discontent Reduction
Insider Decision to Attack Trigger
Insider Forecast of Workplace Discontent
Forecast Time
Time to Increment Workplace Discontent
Effect of Downtime on Workplace Discontent
Fractional Effect of Downtime on Workplace Discontent
Insider Workplace Doscontent Threshold
<Downtime>
Technical Security Level
Technical Security Increment
Technical Security Reduction
Insider Actions to Reduce Technical Security
Init TSL
Desired Technical Security
Management Perception of Technical Security
Insider Actions Severity
Insider Capacity to Reduce Technical Security
Time to Increment Technical Security
Time to Reduce Technical Security Level
Insider Desired Technical Security Reduction
Formal Controls
Fractional Time Increment
Fractional Effect of Downtime on Management Perception of Technical Security
Time to Perceive Technical Security
Mgmt Commitment to Security
<<Downtime>>
Fractional Effect of Formal Controls on Mgmt Time to Perceive Technical Security
Pressure to Grow

Figure 9. Model of Insider Attack on an Information System (Melara et al., 2003)

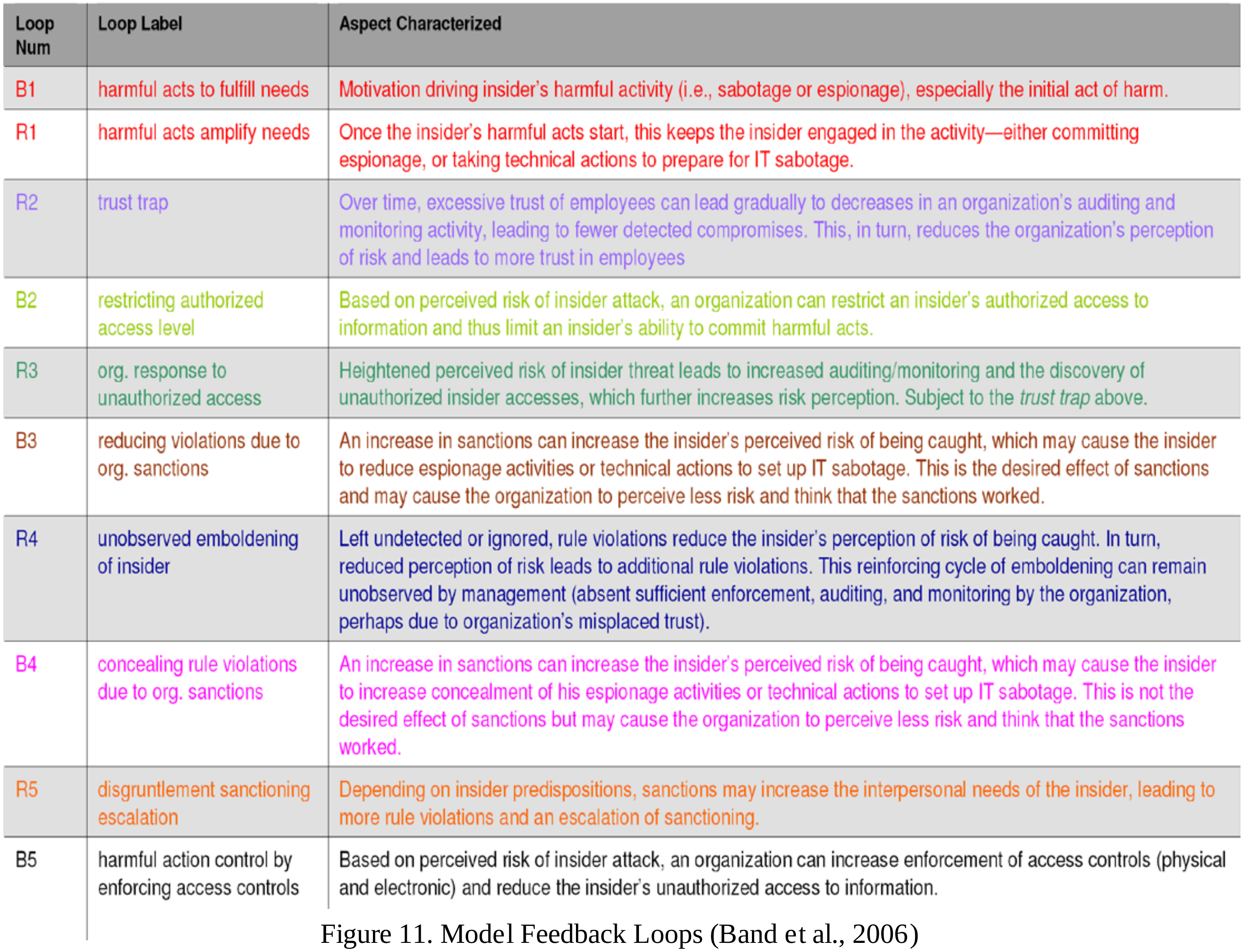
and expectation. It also focuses on both the behavioral and technical indicators that can be monitored and audited. In addition, the model takes into account how an organization might react to such events, through such channels as employee intervention or sanctions. The access paths known and unknown to the organization are also very important elements.

This model also includes balancing and reinforcing loops (described in Figure 11). One example of a balancing loop (labeled 'B3' in Figures 10 and 11) refers to precursory events decreasing because of the issuing of sanctions, which had increased an insider's perceived risk of being caught. As mentioned previously, issuing sanctions can also have an opposite effect. The *disgruntlement sanctioning escalation* loop shows the spiraling effect of this reinforcing loop (labeled 'R5' in Figures 10 and 11). An employee who receives sanctions may become more stressed and disgruntled, which in turn could lead to more precursory events.

2.4.5.4 Espionage Model

The CMU CERT technical staff also developed a system dynamics model entitled "Espionage Model" to look at the variables and relationships present in the espionage component of the insider threat problem (see Figure 12) (Band, et al., 2006). This model also included many factors related to the insider, to include personal needs, disposition, stress, and willingness to commit espionage. Financial needs and greed were very prominent factors as well. On the organizational side, there were variables concerning monitoring and auditing, access paths, discovering of espionage, trust, sanctions, security procedures and awareness training, and culture of reporting suspicious behavior. The model also included influence from the outside in terms of external forces eliciting spies.

Figure 10. Insider IT Sabotage Model (Band et al., 2006)



Loop Num	Loop Label	Aspect Characterized
B1	harmful acts to fulfill needs	Motivation driving insider's harmful activity (i.e., sabotage or espionage), especially the initial act of harm.
R1	harmful acts amplify needs	Once the insider's harmful acts start, this keeps the insider engaged in the activity—either committing espionage, or taking technical actions to prepare for IT sabotage.
R2	trust trap	Over time, excessive trust of employees can lead gradually to decreases in an organization's auditing and monitoring activity, leading to fewer detected compromises. This, in turn, reduces the organization's perception of risk and leads to more trust in employees
B2	restricting authorized access level	Based on perceived risk of insider attack, an organization can restrict an insider's authorized access to information and thus limit an insider's ability to commit harmful acts.
R3	org. response to unauthorized access	Heightened perceived risk of insider threat leads to increased auditing/monitoring and the discovery of unauthorized insider accesses, which further increases risk perception. Subject to the *trust trap* above.
B3	reducing violations due to org. sanctions	An increase in sanctions can increase the insider's perceived risk of being caught, which may cause the insider to reduce espionage activities or technical actions to set up IT sabotage. This is the desired effect of sanctions and may cause the organization to perceive less risk and think that the sanctions worked.
R4	unobserved emboldening of insider	Left undetected or ignored, rule violations reduce the insider's perception of risk of being caught. In turn, reduced perception of risk leads to additional rule violations. This reinforcing cycle of emboldening can remain unobserved by management (absent sufficient enforcement, auditing, and monitoring by the organization, perhaps due to organization's misplaced trust).
B4	concealing rule violations due to org. sanctions	An increase in sanctions can increase the insider's perceived risk of being caught, which may cause the insider to increase concealment of his espionage activities or technical actions to set up IT sabotage. This is not the desired effect of sanctions but may cause the organization to perceive less risk and think that the sanctions worked.
R5	disgruntlement sanctioning escalation	Depending on insider predispositions, sanctions may increase the interpersonal needs of the insider, leading to more rule violations and an escalation of sanctioning.
B5	harmful action control by enforcing access controls	Based on perceived risk of insider attack, an organization can increase enforcement of access controls (physical and electronic) and reduce the insider's unauthorized access to information.

Figure 11. Model Feedback Loops (Band et al., 2006)

Figure 12. Espionage Model (Band et al., 2006)

This model includes the same feedback loops as the Insider IT Sabotage Model (explained in Figure 11).

2.4.5.5 Abstracted Common Model

The CMU CERT technical staff was asked by one of its sponsors, the Defense Personnel Security Research Center, to examine commonalities between the sabotage and espionage categories of insider threat. After creating the Insider IT Sabotage Model and Espionage Model discussed above, the CMU CERT technical staff developed the Abstracted Common Model (see Figure 13). By analyzing case studies from both subcategories, the staff found the six significant commonalties listed below (Band et al., 2006):

1. Malicious insiders had common personal predispositions that led them to commit sabotage or espionage, such as mental health disorders, alcoholism, personality problems (e.g., anger, sense of entitlement, egotism), poor social and decision-making skills, and history of rule conflicts. These personal dispositions resulted in personal needs which in turn led to harmful actions against the organization, motivated by disgruntlement, profit, or opportunity.
2. Often the malicious insiders were affected by stressful events, such as organizational sanctions (to include termination or suspension) and personal events. Furthermore, the insiders' personal predispositions affected how they handled the stressful events. For example, people prone to feeling angry are more likely to become increasingly disgruntled after being issued sanctions. This disgruntlement can lead them to commit additional acts, which may only lead to further sanctions.

3. The malicious insiders exhibited unusual and troublesome behaviors before and during the malicious acts. Examples of these behaviors include being tardy or late for work, arguing with co-workers, performing poorly at their job, violating security policies and procedures, and voicing grievances with or desire to cause harm to the organization.
4. In both subcategories, the malicious insiders conducted technical precursory incidents. Types of incidents include creating unauthorized access paths, accessing documents which they do not need for their job responsibilities, excessive printing or copying of documents, and creating and testing logic bombs. Whether the organizations detected these precursory events was largely due to the level of monitoring and auditing they conducted.
5. The organizations either did not detect or ignored rule violations, whether technical or behavioral. On the technical side, often precursory events were not detected. If they were and sanctions were issued, the malicious insiders many times just did a better job of concealing future incidents. On the behavioral side, often the rule violations were dismissed or ignored, which often emboldened the insiders to continue with such behavior.
6. A deficiency in access controls, either electronic or physical access to resources, helped the malicious insiders to achieve their goal. In some cases, the insiders were given more access than necessary for their job or access was

not decreased once they had been demoted. The organization also may not have practiced the security policies of least privilege and separation of duty.

The Abstracted Common Model also contains the same five balancing and five reinforcing loops as the Insider IT Sabotage Model and Espionage Model (Figure 11).

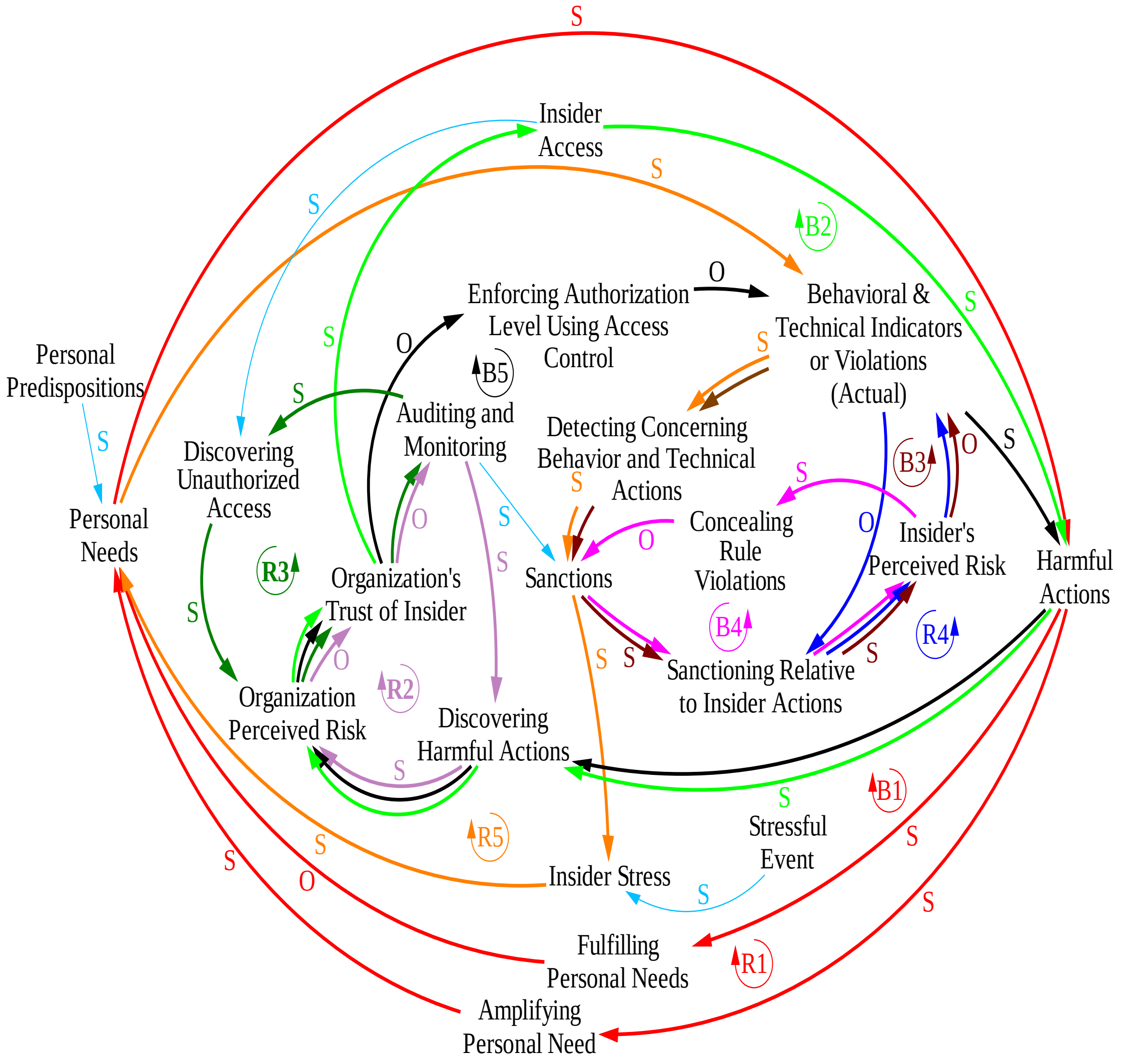

S
Insider Access
S
S
B2
Personal Predispositions
S
S
O
Enforcing Authorization Level Using Access Control
O
Behavioral & Technical Indicators or Violations (Actual)
S
S
B5
S
Auditing and Monitoring
Detecting Concerning Behavior and Technical Actions
S
Discovering Unauthorized Access
S
Personal Needs
O
B3
O
S
S
O
Concealing Rule Violations
O
Insider's Perceived Risk
Harmful Actions
R3
S
Organization's Trust of Insider
S
Sanctions
S
B4
R4
O
S S
Sanctioning Relative to Insider Actions
S
Organization Perceived Risk
R2
Discovering Harmful Actions
S
B1
S
Stressful Event
S
R5
S
S
O
Insider Stress
S
S
Fulfilling Personal Needs
R1
Amplifying Personal Need

Figure 13. Abstracted Common Model (Band et al., 2006)

2.4.5.6 Model of the Insider IT Sabotage Problem

From their development of materials for insider threat workshops and talks they have given at conferences, the CMU CERT technical staff received feedback regarding their system dynamics models. From that feedback, they developed an abstract Model of the Insider IT Sabotage Problem that is more understandable to those who are unfamiliar with system dynamics modeling (Moore et al., 2008) (see Figure 14). They retained the core elements, such as personal disposition, expectation, event, disgruntlement, monitoring, precursors, sanctions, trust, and access paths, but removed some of the smaller, more detailed variables (such as audit quality and technical freedom given to insider). As well, they retained five of the balancing (labeled with a ‘B’) and reinforcing loops (labeled with an ‘R’), which are as follows: expectation escalation (R1), escalation of disgruntlement (R2), unobserved emboldening of insider (R3), trust trap (R4), and intended effects of sanctions (B1).

2.5 Summary

This chapter examined the variables that previous research has identified in the insider threat problem, to include those attributed to the insider and to the organization. To further explain these and see how they can come into play, the attacks performed by Robert Hanssen and Timothy Lloyd were described. Additionally, insider threat models from previous research were presented to depict the relationships among these variables. In order to better understand these models and those developed for this research, background information was included on logical data and system dynamics modeling.

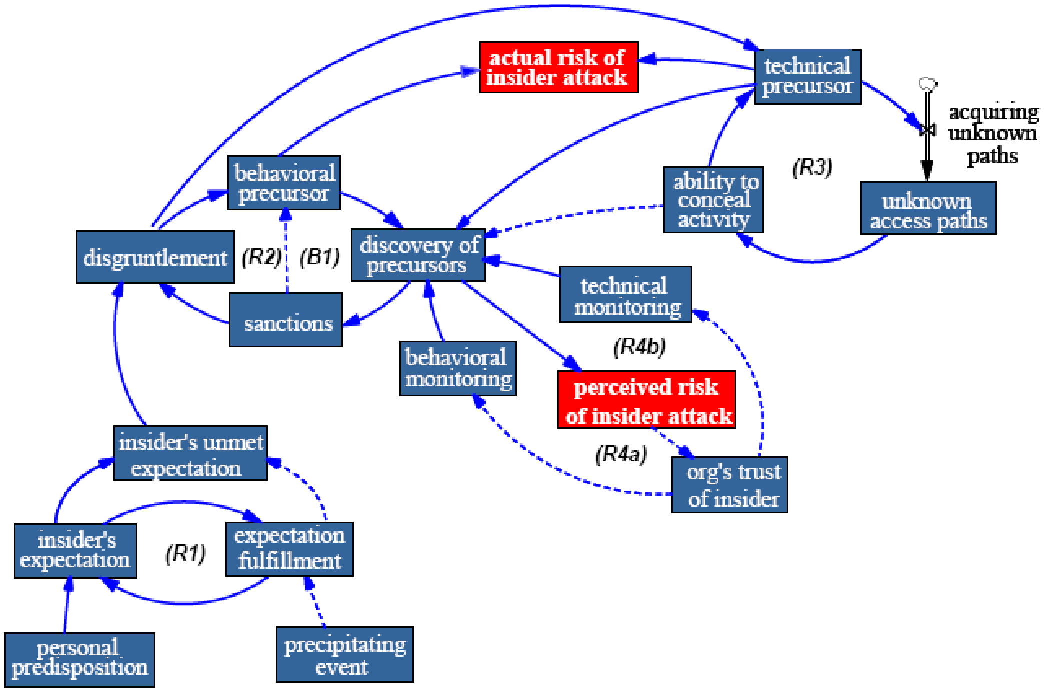

actual risk of insider attack
technical precursor
acquiring unknown paths
unknown access paths
(R3)
ability to conceal activity
behavioral precursor
disgruntlement
(R2)
(B1)
discovery of precursors
sanctions
technical monitoring
(R4b)
behavioral monitoring
perceived risk of insider attack
(R4a)
org's trust of insider
insider's unmet expectation
insider's expectation
(R1)
expectation fulfillment
personal predisposition
precipitating event

Figure 14. Model of the Insider IT Sabotage Problem (Moore et al., 2008)

In the next chapter, the logical data and system dynamics models created for this research are presented. There is also a discussion of why the CMU CERT technical staff's Abstracted Common Model was chosen as the most relevant to the USAF and therefore used as the basis for the model to be used in the policy review. Lastly, the chapter will explain the additional variables that were incorporated, resulting in this research's Insider Threat Model for Sabotage and Espionage.

III. Insider Threat Modeling

3.1 Overview

To ensure the most appropriate model was used for the review of USAF policy, this research first modeled the problem as a way to tie the many variables together. In this chapter, the logical data and system dynamics models that were first developed for this research are described in detail, to include the models' entities, attributes, relationships, and feedback loops. Afterwards, there is an explanation of why the CMU CERT technical staff's Abstracted Common Model was selected as the basis for this research's Insider Threat Model for Sabotage and Espionage. The reasoning behind incorporating motivations, organizational priorities, and social networks is also presented.

3.2 Logical Data Model

To better understand the insider threat problem, variables from the various insider threat models were incorporated into this research's Insider Threat Logical Data Model. The attributes of the entities were listed out, as well as the relationships between the entities. These entities were then tied together with the risk assessment elements (threat, vulnerability, likelihood, impact, and risk). By examining their organizations through the lens of this model, managers can identify what elements in their organization may be putting them at risk of an insider attack. Hopefully, they can then work to decrease the vulnerabilities, threats, or both. As mentioned in the last chapter, this model was inspired by Tuglular's (2000) structural approach which outlined the elements and attributes which play a role in an insider attack.

To make the model easier to read, Figure 15 includes all the entities and relationships but excludes the attributes. The entities in the yellow-highlighted area (Area 1) are attributed to the insider, and those in the green-highlighted are related to the organization (Area 2). The risk management entities are shaded in magenta (Area 3). Figures 16 through 20 depict portions of the model with all attributes and keys for the included entities.

3.2.1 Entities of the Insider Threat Logical Data Model

This next section outlines each of the entities included in the Insider Threat Logical Data Model to include their attributes.

3.2.1.1 Organization

There are elements of the organization itself that can play a role in determining whether it is at risk of an insider attack (see Figures 15 and 16). These include the type of business with which the organization is involved (e.g., military, education, or customer service), what it considers its priorities (e.g., reputation or profits) (Rich et al., 2005), and its propensity to trust its employees (McKnight et al., 1998).

3.2.1.2 Control

The controls an organization chooses to implement to detect and protect it from insider attacks are also important entities to examine (see Figures 15, 16, and 19). These controls usually fall into one of the following three categories: technical, formal, or informal (Melara et al., 2003); most likely an organization implements controls from all three categories. The type of control can vary from monitoring (technical) to issuing sanctions (formal) (Cappelli et al., 2007) to organizational culture (informal) (Melara et al., 2003).

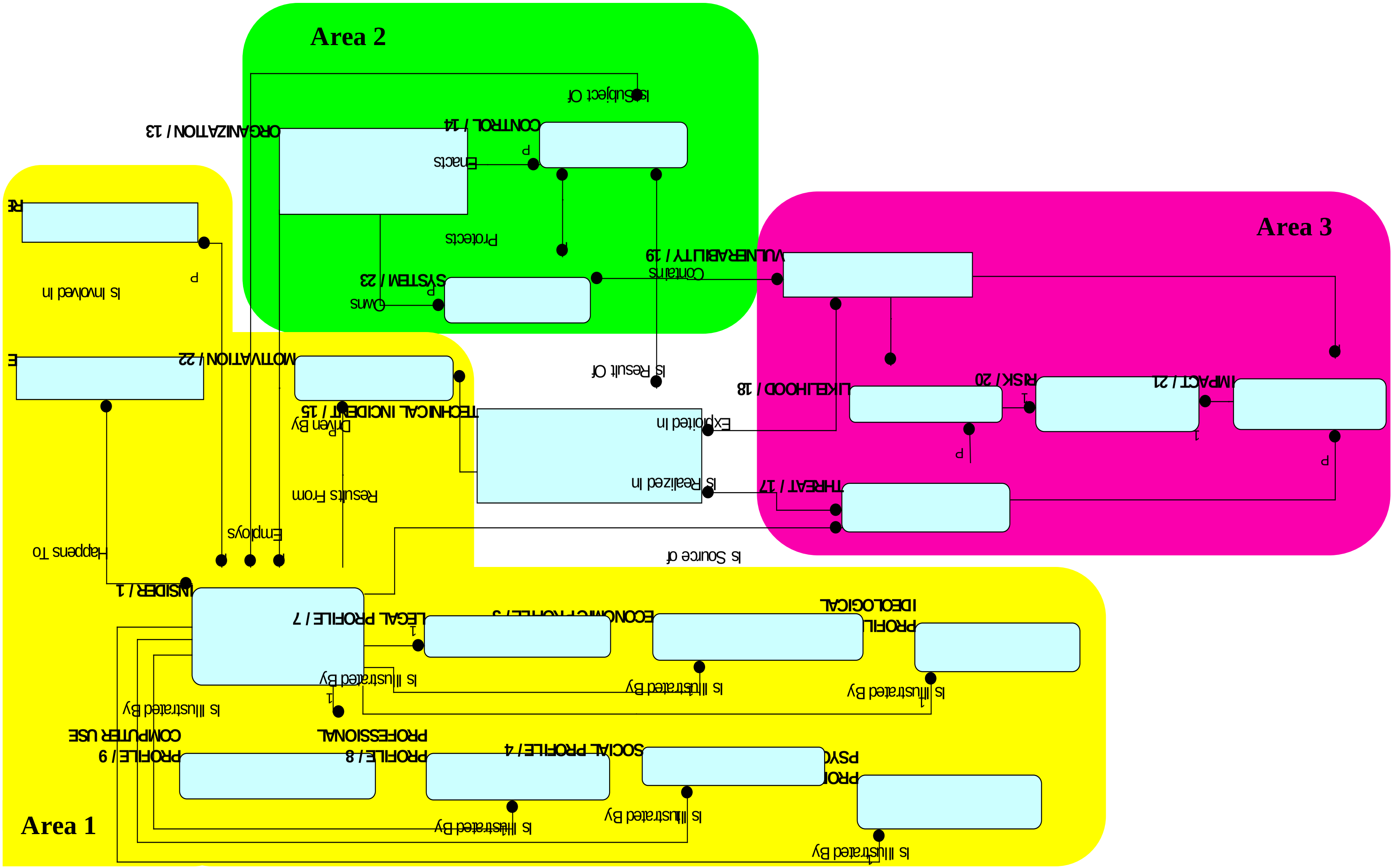

Area 1
Area 2
Area 3
INSIDER / 1
PSYCHOLOGICAL PROFILE
SOCIAL PROFILE / 4
ECONOMIC PROFILE / 5
IDEOLOGICAL PROFILE
LEGAL PROFILE / 7
PROFESSIONAL PROFILE / 8
COMPUTER USE PROFILE / 9
ORGANIZATION / 13
CONTROL / 14
TECHNICAL INCIDENT / 15
THREAT / 17
LIKELIHOOD / 18
VULNERABILITY / 19
RISK / 20
IMPACT / 21
MOTIVATION / 22
SYSTEM / 23
Is Illustrated By
Is Source of
Is Realized In
Exploited In
Is Result Of
Contains
Protects
Owns
Enacts
Is Subject Of
Employs
Results From
Driven By
Happens To
Is Involved In
P
1

Figure 15. Insider Threat Logical Data Model

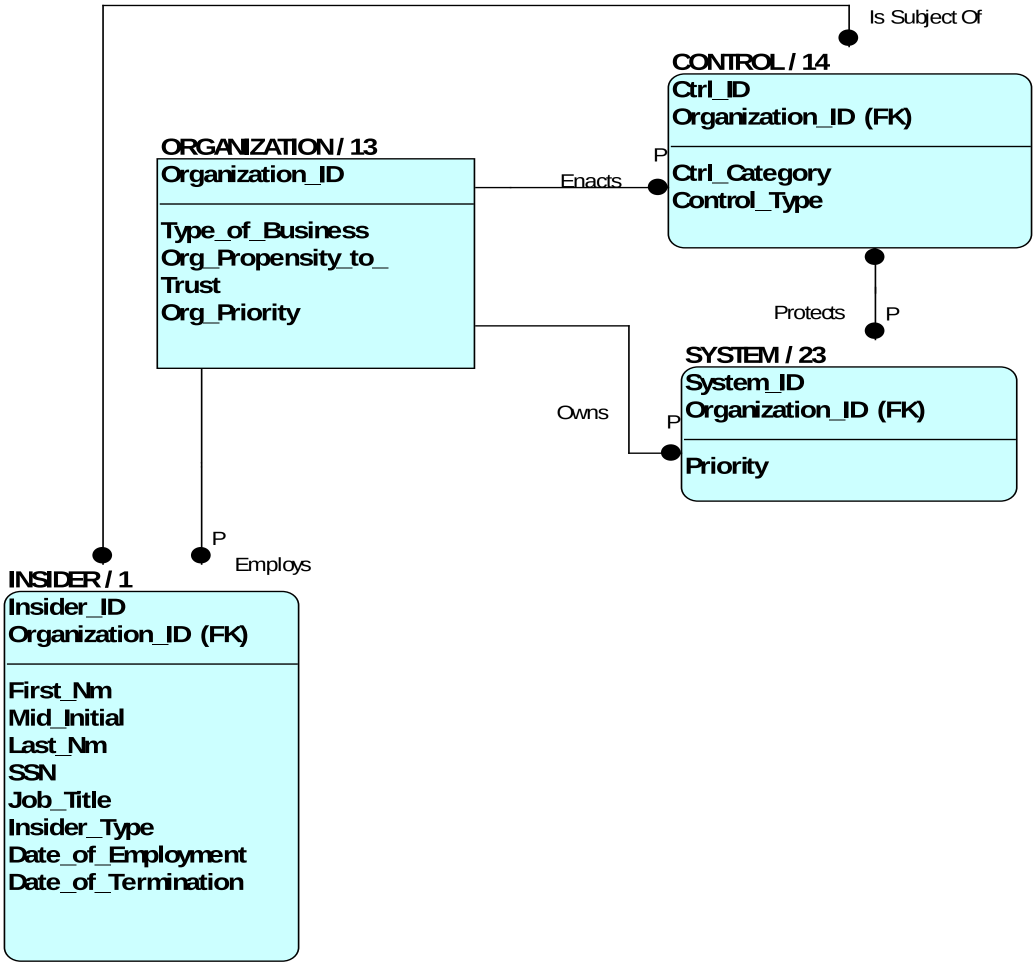

Is Subject Of
CONTROL / 14
Ctrl_ID
Organization_ID (FK)
Ctrl_Category
Control_Type
ORGANIZATION / 13
Organization_ID
Type_of_Business
Org_Propensity_to_
Trust
Org_Priority
Enacts
P
Protects
P
SYSTEM / 23
System_ID
Organization_ID (FK)
Priority
Owns
P
P
Employs
INSIDER / 1
Insider_ID
Organization_ID (FK)
First_Nm
Mid_Initial
Last_Nm
SSN
Job_Title
Insider_Type
Date_of_Employment
Date_of_Termination

Figure 16. Organization and Related Entities

3.2.1.3 System

Having an inventory of the organization's systems is an important element in mitigating any type of security risk (Pipkin, 2000) (see Figures 15, 16, and 19). The organization needs to know what resources it has, as well as prioritize them based on their value to the company. A system's priority can help an organization determine how much money and time it is willing to invest in order to protect it.

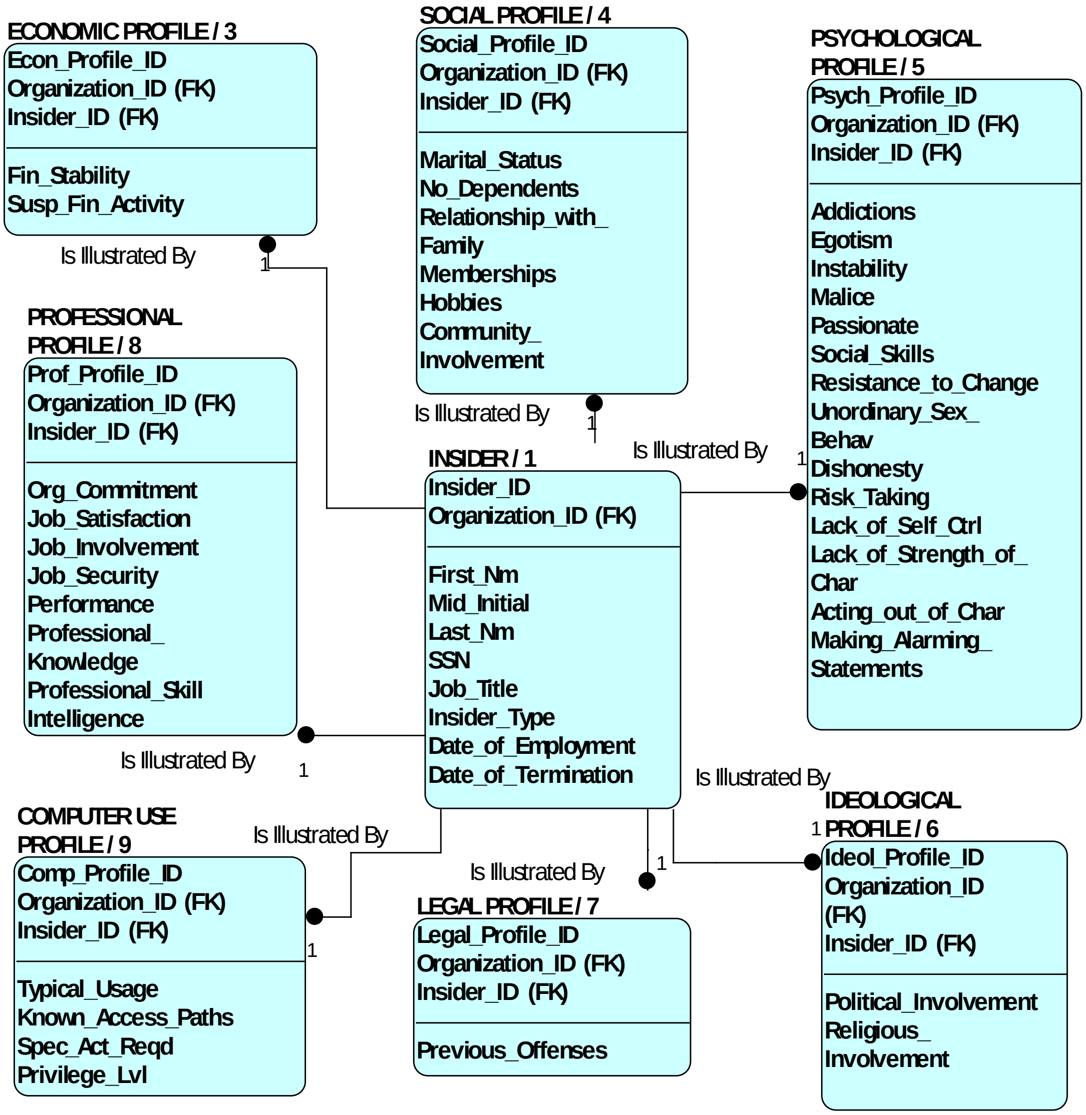

ECONOMIC PROFILE / 3
Econ_Profile_ID
Organization_ID (FK)
Insider_ID (FK)
Fin_Stability
Susp_Fin_Activity
SOCIAL PROFILE / 4
Social_Profile_ID
Organization_ID (FK)
Insider_ID (FK)
Marital_Status
No_Dependents
Relationship_with_
Family
Memberships
Hobbies
Community_
Involvement
PSYCHOLOGICAL
PROFILE / 5
Psych_Profile_ID
Organization_ID (FK)
Insider_ID (FK)
Addictions
Egotism
Instability
Malice
Passionate
Social_Skills
Resistance_to_Change
Unordinary_Sex_
Behav
Dishonesty
Risk_Taking
Lack_of_Self_Ctrl
Lack_of_Strength_of_
Char
Acting_out_of_Char
Making_Alarming_
Statements
PROFESSIONAL
PROFILE / 8
Prof_Profile_ID
Organization_ID (FK)
Insider_ID (FK)
Org_Commitment
Job_Satisfaction
Job_Involvement
Job_Security
Performance
Professional_
Knowledge
Professional_Skill
Intelligence
INSIDER / 1
Insider_ID
Organization_ID (FK)
First_Nm
Mid_Initial
Last_Nm
SSN
Job_Title
Insider_Type
Date_of_Employment
Date_of_Termination
COMPUTER USE
PROFILE / 9
Comp_Profile_ID
Organization_ID (FK)
Insider_ID (FK)
Typical_Usage
Known_Access_Paths
Spec_Act_Reqd
Privilege_Lvl
LEGAL PROFILE / 7
Legal_Profile_ID
Organization_ID (FK)
Insider_ID (FK)
Previous_Offenses
IDEOLOGICAL
PROFILE / 6
Ideol_Profile_ID
Organization_ID
(FK)
Insider_ID (FK)
Political_Involvement
Religious_
Involvement
Is Illustrated By
1
Is Illustrated By
1
Is Illustrated By
1
Is Illustrated By
1
Is Illustrated By
1
Is Illustrated By
1
Is Illustrated By
1
Is Illustrated By
1

Figure 17. Insider and Profile Entities

3.2.1.4 Insider

The people potentially responsible for insider attacks must be tracked (see Figures 15 through 19). Basic information includes name, social security number, job title, date of employment, date of termination, and insider type (current or former employee, service providers, consultants, or contractors) (CSO, 2007).

3.2.1.5 Psychological Profile

As much as possible, it is beneficial to have a psychological profile on all insiders (see Figures 15 and 17). Obviously, this is more difficult for service providers, consultants, or contractors, but some personality traits and behaviors may be exhibited as insiders work with the organization. Though there does not exist a profile for malicious insiders, the following traits and behaviors have historically been possessed or exhibited by malicious insiders: egotism, instability, malice, passion, dishonesty, risk taking, lack of self control, lack of strength of character, poor social skills, addictions, (Tuglular, 2000), acting out of character, making alarming statements (Puleo, 2006), resistance to change (Robbins and Judge, 2008), and unordinary sexual behavior (Under Secretary for Management, 2006).

3.2.1.6 Legal Profile

It is beneficial to know the criminal record of all insiders, to include previous offenses (see Figures 15 and 17). Individuals who have broken the law in the past may be more inclined to do so again (Under Secretary for Management, 2006).

3.2.1.7 Computer Use Profile

It is important to understand the typical computer usage patterns of each insider, to include the following: password failure pattern (Tuglular, 2000), documents read versus written ratio, documents printed, printing other users' documents, number of databases accessed, latest work end time, and earliest work start time (Laird and Rickard, 2005) (see Figures 15 and 17). If while monitoring insiders, it is discovered that they are suddenly participating in activities that do not fit their normal pattern, the organization should be concerned and look into the situation. It is also important to know of any special activities, such as high usage of the file transfer protocol (FTP) or access to unusual websites, which they legitimately need for their job. Awareness of these unique activities can help prevent the organization from examining false positives. It is essential to know what privilege level the insiders have on the network and what resources they can access (Cappelli et al., 2007).

3.2.1.8 Social Profile

It is beneficial to have insight into each insider's personal life (see Figures 15 and 17). Once a baseline is established, an organization should be on the lookout for any changes, such as withdrawal from usual hobbies or social groups, as they can be signs of the occurrence of a stressful event, such as a divorce. The recommended attributes to track are marital status, number of dependents, relationship with family, memberships, hobbies, and community involvement (Tuglular, 2000).

3.2.1.9 Economic Profile

Historically, economic factors have played a major role in motivating insiders to commit malicious acts (Tuglular, 2000) (see Figures 15 and 17). In terms of sabotage, insiders may feel they have not received the promotion or raise that they think they deserve. Individuals who are in financial trouble are more likely to find espionage an attractive option. Attributes of this entity include insiders' suspicious financial activity and financial stability or security.

3.2.1.10 Ideological Profile

It is also important to have insight into insiders' roles in religion and politics (Tuglular, 2000) (see Figures 15 and 17). Similar to the *Social Profile* entity, it is valuable to establish baselines and then watch for any changes, such as an individual's sudden withdrawal from or new membership in a church. Involvement in a new religious or political organization could also have social or economic effects.

3.2.1.11 Professional Profile

Insiders' feelings towards and behavior in the workplace are also important factors in the insider threat problem (see Figures 15 and 17). Again, some of these attributes may be kept internally by the insiders, though others could be expressed to co-workers or supervisors. To capture an accurate picture of an insider, the following factors should be identified: job satisfaction, organizational commitment, job involvement (Robbins and Judge, 2008), job security, job performance (e.g., absenteeism and not able to meet deadlines or handle appropriate workload) (Puleo, 2006), professional knowledge, professional skills, and intelligence (Tuglular, 2000).

3.2.1.12 Event

Events such as change in marital status or demotion can often be triggers for deviant behavior in the workplace (see Figures 15 and 18). The events can either increase the insiders' stress or decrease their expectation fulfillment. Both of these can lead to an increase in insiders' personal needs, which can in turn bring about additional harmful actions (Band et al., 2006). The event can be nationwide (e.g., recession), organization-wide (e.g., restructuring, mergers, personnel cuts, or relocation), or at an individual level (e.g., death in the family, health issues, or change in supervisor) (Cappelli et al., 2007).

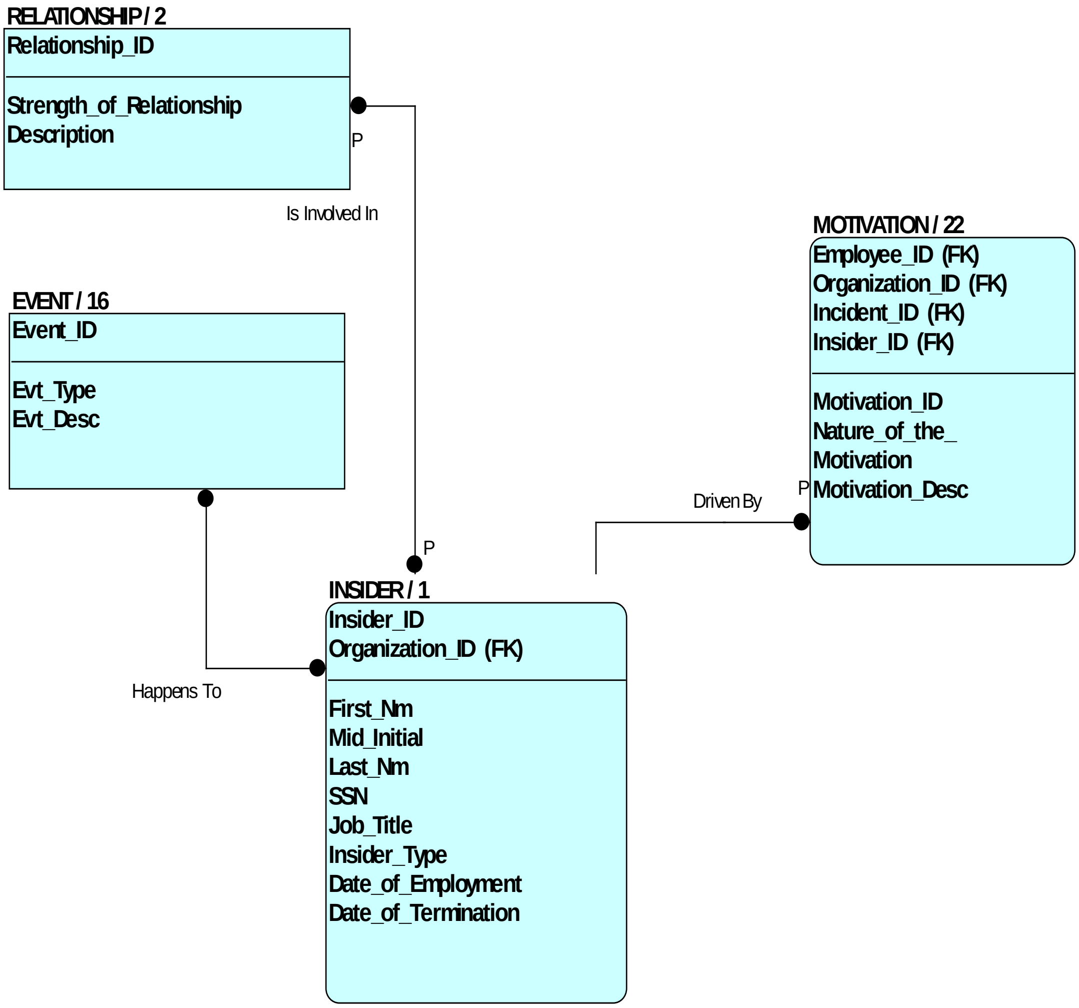

RELATIONSHIP / 2
Relationship_ID
Strength_of_Relationship
Description
P
Is Involved In
EVENT / 16
Event_ID
Evt_Type
Evt_Desc
MOTIVATION / 22
Employee_ID (FK)
Organization_ID (FK)
Incident_ID (FK)
Insider_ID (FK)
Motivation_ID
Nature_of_the_
Motivation
Motivation_Desc
P
Driven By
P
INSIDER / 1
Insider_ID
Organization_ID (FK)
Happens To
First_Nm
Mid_Initial
Last_Nm
SSN
Job_Title
Insider_Type
Date_of_Employment
Date_of_Termination

Figure 18. Insider and Related Entities

3.2.1.13 Relationship

Insiders' social ties within the organization can either lead to or prevent them from participation in deviant behavior (see Figures 15 and 18). If insiders have strong ties with co-workers, they are more reluctant to commit deviant behavior in the workplace that could jeopardize these relationships. On the other hand, if insiders are in relationships with others who are committing malicious acts, they may be more inclined to follow suit (Theoharidou et al., 2005).

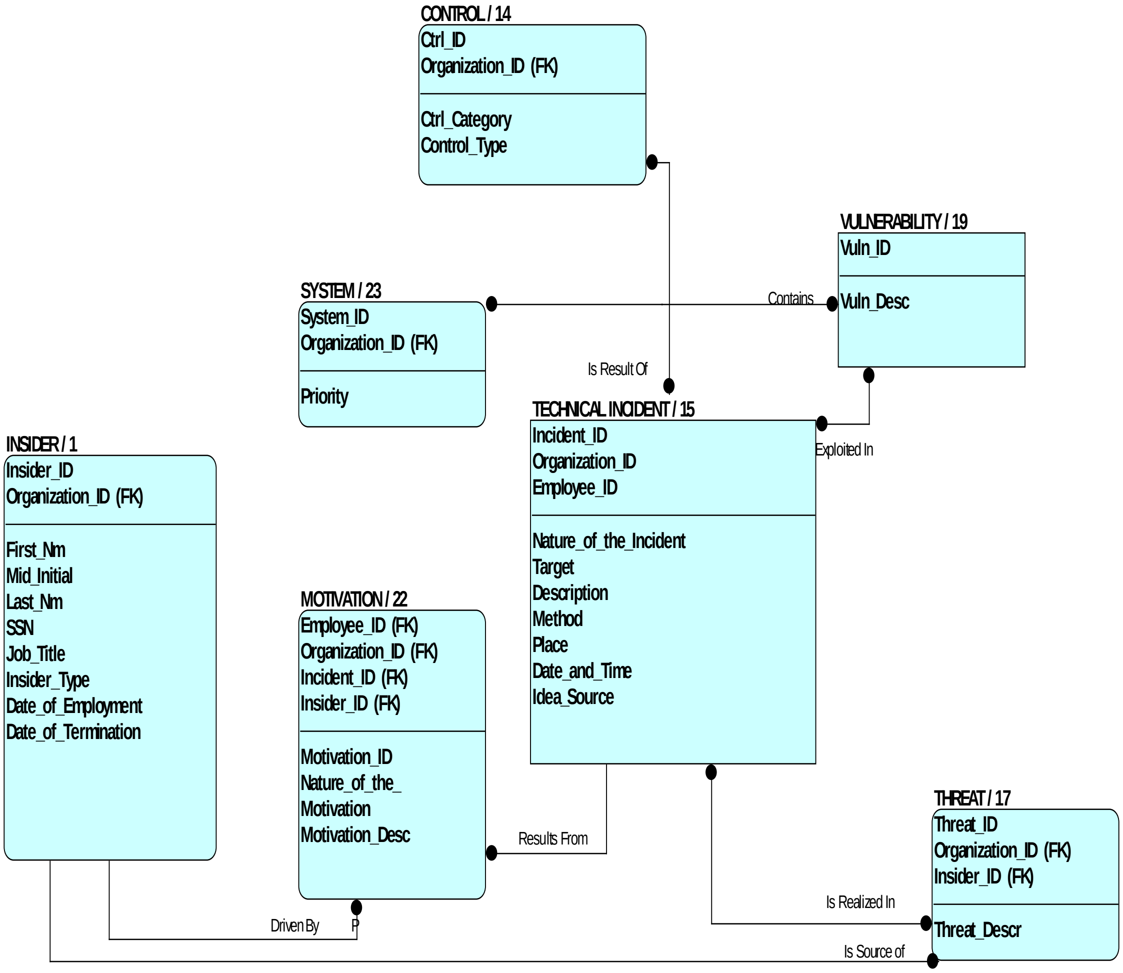

CONTROL / 14
Ctrl_ID
Organization_ID (FK)
Ctrl_Category
Control_Type
VULNERABILITY / 19
Vuln_ID
Vuln_Desc
SYSTEM / 23
System_ID
Organization_ID (FK)
Priority
Contains
Is Result Of
TECHNICAL INCIDENT / 15
Incident_ID
Organization_ID
Employee_ID
Nature_of_the_Incident
Target
Description
Method
Place
Date_and_Time
Idea_Source
Exploited In
INSIDER / 1
Insider_ID
Organization_ID (FK)
First_Nm
Mid_Initial
Last_Nm
SSN
Job_Title
Insider_Type
Date_of_Employment
Date_of_Termination
MOTIVATION / 22
Employee_ID (FK)
Organization_ID (FK)
Incident_ID (FK)
Insider_ID (FK)
Motivation_ID
Nature_of_the_
Motivation
Motivation_Desc
Results From
THREAT / 17
Threat_ID
Organization_ID (FK)
Insider_ID (FK)
Threat_Descr
Is Realized In
Driven By
P
Is Source of

Figure 19. Incident and Related Entities

3.2.1.14 Motivation

All malicious insiders are motivated by something (see Figures 15, 18, and 19). Common motives in criminal behavior are money and revenge (Casey, 2004). Similar to psychological characteristics, insiders' motivations may not be evident to anyone else. If they do divulge information regarding the nature of their motivation, then it should be recorded.

3.2.1.15 Incident

If a technical incident does occur, many details should be investigated and recorded, especially since it may be a precursor to a larger, more damaging attack. The organization should try to determine the nature of the incident (intentional destruction, detrimental misuse, dangerous tinkering, or naive mistake) (see Figures 15 and 19). It is important to note that acts that seem harmless could be malicious insiders' attempts to test the security controls (Stanton, et al., 2005). A description of each incident should be recorded (for example, accessing unauthorized websites, installing unauthorized software, or creating covert channels) (Mills et al., 2009). Additionally, it would be beneficial to know where the insider got the idea for the attack, (e.g., from Internet research or another employee), as well as the target, method, date, time, and place (e.g., at work or via virtual private network [VPN]) (Tuglular, 2000).

3.2.1.16 Threat

A threat is the potential of a threat-source (in this case a malicious insider) to trigger or exploit a vulnerability (see Figures 15, 19, and 20). Examples include information disclosure and alteration of software. Identifying potential threats is an important step in the risk management process; this activity should be completed by all organizations (Stoneburner et al., 2002).

3.2.1.17 Vulnerability

A vulnerability is a flaw or weakness in a system within the organization that can be triggered or exploited (see Figures 15, 19, and 20). Just as an organization needs to identify potential threats, it should also determine what its vulnerabilities are, especially since this is what adversaries do in order to increase their likelihood of success. Examples of vulnerabilities include unpatched systems and terminated employees still having access to company resources (Stoneburner et al., 2002).

3.2.1.18 Likelihood

In risk management, likelihood is the probability that a threat will be successfully exercised against a vulnerability (see Figures 15 and 20). For each threat-vulnerability pair, an organization should determine if they think the likelihood is low, moderate, or high (Elky, 2006).

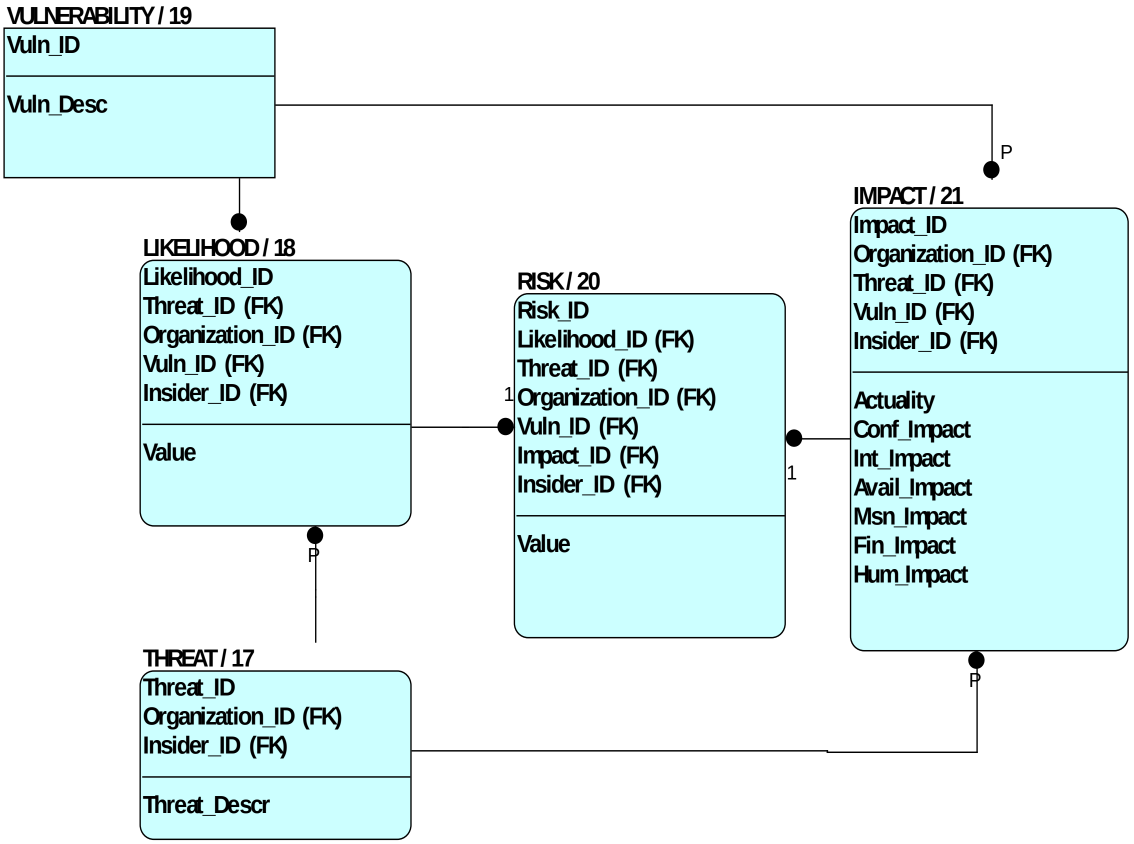

VULNERABILITY / 19
Vuln_ID
Vuln_Desc
P
IMPACT / 21
Impact_ID
Organization_ID (FK)
Threat_ID (FK)
Vuln_ID (FK)
Insider_ID (FK)
Actuality
Conf_Impact
Int_Impact
Avail_Impact
Msn_Impact
Fin_Impact
Hum_Impact
LIKELIHOOD / 18
Likelihood_ID
Threat_ID (FK)
Organization_ID (FK)
Vuln_ID (FK)
Insider_ID (FK)
Value
RISK / 20
Risk_ID
Likelihood_ID (FK)
Threat_ID (FK)
Organization_ID (FK)
Vuln_ID (FK)
Impact_ID (FK)
Insider_ID (FK)
Value
1
1
P
THREAT / 17
Threat_ID
Organization_ID (FK)
Insider_ID (FK)
Threat_Descr
P

Figure 20. Risk and Related Entities

3.2.1.19 Impact

In risk management, the impact of a threat-vulnerability pair is usually the combination of losses in terms of confidentiality, integrity, availability, as well as effects on mission capability, assets, and human life (see Figures 15 and 20). Organizations must determine for their particular organization what the predicted impact will be, usually using the categories of low, moderate, or high (Elky, 2006).

3.2.1.20 Risk

Risk is determined by analyzing the predicted likelihood and impact of the threat exercising the vulnerability (see Figures 15 and 20). Usually this is measured qualitatively as low, medium, high, or critical. The risk management process assists organizations in deciding which threat-vulnerability pairs to address first (Mills et al., 2009).

3.2.2 Relationships in the Insider Threat Logical Data Model

This section outlines the relationships included in the Insider Threat Logical Data Model (see Figure 15).

- *An Organization enacts Controls.*

  The management of the organization is responsible for developing, enacting, and enforcing the controls (see Figure 16).

- *An Organization owns Systems.*

  The organization owns the systems and the information in them, and therefore, it is responsible for protecting those systems (see Figure 16).

- *An Organization employs Insiders.*

  The management of the organization is the responsible for hiring, monitoring, evaluating, disciplining, promoting, and terminating employees (see Figure 16).

- *An Insider is the subject of a Control.*

  Controls can be directed at particular insiders, for example system administrators. Additionally, if an insider is issued a sanction, that individual is the subject of the control (see Figure 16).

- *An Insider is illustrated by a Psychological Profile.*

  Each insider has a one psychological profile, which may be unique within the organization (see Figure 17).

- *An Insider is illustrated by a Legal Profile.*

  Each insider has a one legal profile, which may be unique within the organization (see Figure 17).

- *An Insider is illustrated by a Computer Use Profile.*

  Each insider has a one computer use profile, which may be unique within the organization (see Figure 17).

- *An Insider is illustrated by a Social Profile.*

  Each insider has a one social profile, which may be unique within the organization (see Figure 17).

- *An Insider is illustrated by an Economic Profile.*

  Each insider has a one economic profile, which may be unique within the organization (see Figure 17).

- *An Insider is illustrated by an Ideological Profile.*

  Each insider has a one ideological profile, which may be unique within the organization (see Figure 17).

- *An Insider is illustrated by a Professional Profile.*

  Each insider has a one professional profile, which may be unique within the organization (see Figure 17).

- *An Insider is involved in Relationships.*

  Insiders are involved in a relationship with their supervisors. They may be involved in many other relationships with co-workers as well (see Figure 18).

- *An Event happens to an Insider.*

  Insiders are positively or negatively affected by nationwide, organization-wide, and individual-level events (see Figure 18).

- *An Insider is driven by Motivations.*

  Insiders commit malicious acts due to at least one of the various motivational factors (see Figure 18).

- *A System contains a Vulnerability.*

  An individual system may have one or more vulnerabilities. Also, a single vulnerability can be present in and affect multiple systems or possibly the organization as a whole (see Figure 19).

- *An Insider is the source of a Threat.*

  Within this discussion of insider threat, all the threat-sources are insiders (see Figure 19).

- *A Technical Incident results from a Motivation.*

  Insiders have at least one source of motivation for committing a technical incident (see Figure 19).

- *A Vulnerability is exploited in a Technical Incident.*

  A technical incident is the pairing of a threat to a vulnerability (see Figure 19).

- *A Threat is realized in a Technical Incident.*

  A technical incident is the pairing of a threat to a vulnerability (see Figure 19).

- *A Control is a result of a Technical Incident.*

  A control may be introduced into the organization after the occurrence of an incident, whether it is new company-wide policy or a sanction issued to the insider who was the source (see Figure 19).

- *A Threat and Vulnerability have a Likelihood.*

  A threat-vulnerability pair has a resulting likelihood (see Figure 20).

- *A Threat and Vulnerability have an Impact.*

  A threat-vulnerability pair has a resulting impact (see Figure 20).

- *A Likelihood and Impact have a Risk value.*

  A likelihood-impact pair has a risk value (see Figure 20).

3.3 System Dynamics Model

Once the logical data model was completed, a system dynamics model was developed to explain how these entities affected each other (i.e., positively or negatively) and ultimately how they may increase or decrease a system's level of risk in terms of the insider threat problem. As mentioned in the last chapter, this research's Insider Threat

System Dynamics Model (see Figure 21) was greatly inspired by the CMU CERT technical staff's abstract Model of the Insider IT Sabotage Problem (Moore et al., 2008). This model was chosen as it included more of the entities and attributes included in the Insider Threat Logical Data Model than any of the other models, such as personal characteristics, organizational controls, trust, and events. Many of the variables in the Insider Threat System Dynamics Model were purposefully named to provide consistency with the CMU model.

This next section describes the two variables at the heart of this model, *Organizational Controls* and *Insider's Motivation to Commit Malicious Act*, to include the interactions they have with each other as well as their relationships with the model's other variables. The incorporation of the risk management variables and the feedback loops within the model are also explained. This model uses a '+' sign for relationships with a positive correlation and '-' for those with a negative correlation.

3.3.1 Organizational Controls

An organization's priorities play a role in how much it invests in controls, such as monitoring and training. An organization that prioritizes reputations often invests more, while one that prioritizes profits invests less (Rich et al., 2005). If the organization prioritizes a particular system, it usually spends more to protect it (Mills et al., 2009). If an organization has a low amount of trust in its employees, it often spends more money on controls as it feels an attack is likely. Similarly, if an organization begins to discover precursory incidents, it most likely increases controls, for example additional monitoring or issuing of sanctions (Moore et al., 2008).

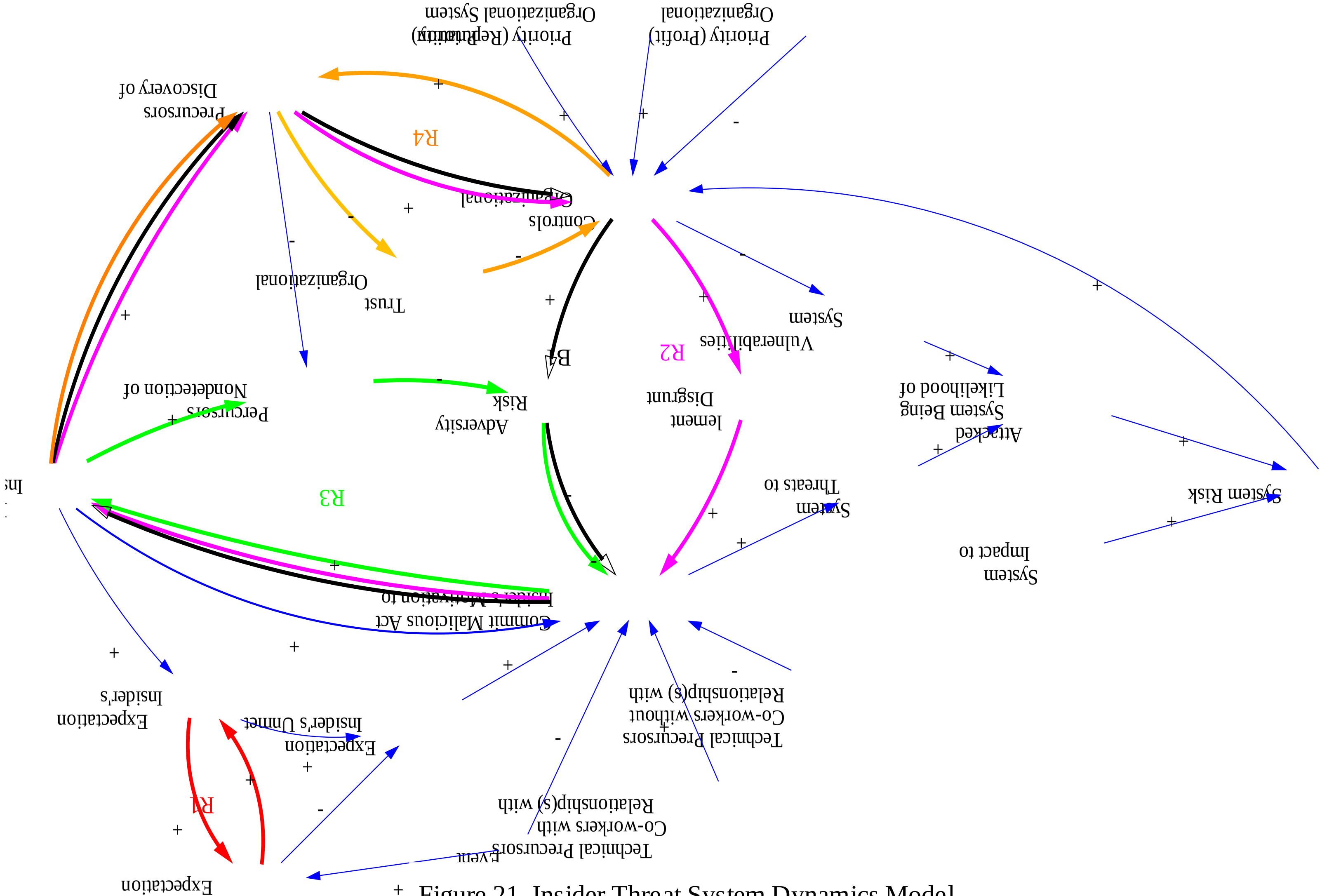

Organizational
Priority (Profit)
Organizational System
Priority (Reputation)
Discovery of
Precursors
Organizational
Controls
Organizational
Trust
Nondetection of
Percursors
Adversity
Risk
Disgrunt
lement
System
Vulnerabilities
Likelihood of
System Being
Attacked
System Risk
Impact to
System
Threats to
System
Insider's Motivation to
Commit Malicious Act
Relationship(s) with
Co-workers without
Technical Precursors
Relationship(s) with
Co-workers with
Technical Precursors
Event
Insider's Unmet
Expectation
Insider's
Expectation
Fulfillment
Expectation
R1
R2
R3
R4
B4
+
-

Figure 21. Insider Threat System Dynamics Model

3.3.2 Insider's Motivation to Commit Malicious Act

Insiders' motivation to commit a malicious act can be increased by relationships with co-workers who are also committing such acts. These co-workers can serve as poor role models. On the other hand, relationships with co-workers who are not themselves committing malicious acts can decrease the motivation of insiders, as they would not want to jeopardize these relationships (Theoharidou et al., 2005). Negative events, such as change in marital status, could also increase insiders' motivation to attack (Puleo, 2006). A negative event can also lead to a decrease in insiders' expectation fulfillment, which increases their unmet expectation level and subsequently their motivation to act (Moore et al., 2008).

Insider precursors, in terms of legal, professional, and psychological traits and behaviors, can also increase insiders' motivation. For example, insiders who have had legal problems in the past, are egotistical, feel they deserve promotions (Tuglular, 2000), and are dissatisfied with their jobs (Puleo, 2006) could be more motivated to attack their company. The psychological disposition of insiders may also lead them to have naturally higher expectations of the access and recognition they should receive at work. As mentioned earlier, if expectations are not met, their motivation to attack can be increased (Moore et al., 2008).

3.3.3 Relationships Between Insider's Motivation and Organizational Controls

Organizational controls can have two very different affects on insiders' motivation to act maliciously. If there are many controls in place to monitor and audit employee activity, then the risk adversity of insiders often is increased, which in turn decreases their motivation to act as they feel that the likelihood of being detected is greater. On the other hand, if upset employees are issued sanctions (an increase in organizational controls), they may simply become more disgruntled and more likely to act (Cappelli and Moore, 2008).

3.3.4 Incorporation of Risk Management

In risk management, as either the number of threats or vulnerabilities to a system increase so does the likelihood of an attack to that system. As either the likelihood or impact of an attack to a system increases so does the risk to that system. Since the threats come from insiders, as their motivation increases so does the threat level. Since organizational controls are enacted to protect the systems, as the number of controls increases, the number of vulnerabilities should decrease. Additionally, if an organization recognized that a particular system had a high risk level, it would likely increase the number of controls in place to protect that system.

3.3.5 Feedback Loops

To align with the Model of the Insider IT Sabotage Problem (Moore et al., 2008), the model in this paper incorporated the same feedback loops, described next.

- *Expectation Escalation* (labeled R1- shown in red on the model)

  If insiders have their expectations fulfilled, then often that simply raises their level of expectation for the future. This is a reinforcing loop that could spiral out of control.

- *Escalation of Disgruntlement* (labeled R2- shown in pink on the model)

  If insiders are committing precursory technical incidents or displaying unusual behavior, these are either discovered or go undetected. If precursors are discovered, then organizational controls, such as monitoring and the issuing of sanctions, are increased. This increase of organizational controls can increase the insiders' disgruntlement. In turn, this can increase their motivation to commit an act and lead to more precursory incidents or behaviors. Again this is a reinforcing loop which can continuously escalate.

- *Intended Effects of Sanctions* (labeled B1- shown in black on the model)

  The issuing of sanctions and increase of other organizational controls can have a very different effect on insiders. If these controls increase insiders' risk adversity, they may actually become less motivated to attack since they feel it is likely that they will be detected again. This decrease in motivation can actually lessen the number of future precursory incidents or behaviors. This is a balancing loop which works towards reaching the goal state of no or few precursors.

- *Unobserved Emboldening of Insider* (labeled R3- shown in green on the model)

  If precursors go undetected, the insiders' risk adversity is lowered and their motivation to act again is increased as they feel they could get away with malicious activity. This often leads to additional acts. This is a reinforcing loop; if the insiders' actions continue to go undetected, they will continue to act.

- *Trust Trap* (labeled R4- shown in orange on the model)

  If an organization has low trust in its employees, it usually invests more in controls, such as monitoring and auditing. With more controls in place, the likelihood of an incident being detected is greater. As more incidents are detected, the organization's trust lowers even more, leading to additional controls. This is another reinforcing loop.

3.4 Selection of the Abstracted Common Model

After the development of the logical data and system dynamics models, the final step before conducting the review of the USAF policies was to develop the model that would be used for comparison. It was decided that first a previously published model would be selected as the basis. From the review of the models described in Chapter II, the Abstracted Common Model was chosen as the most relevant and understandable for the audience of USAF leaders and supervisors. Both insider espionage and sabotage are concerns of the USAF; therefore, a model that focuses on the commonalties of these two problem areas is ideal. Mitigating insider threat is a difficult and still fairly new problem. Measures that can help prevent two types of insider threat are therefore very attractive as they guide organizations as they begin to invest in fighting against the problem (Cappelli and Moore, 2008). In addition, the fact that this model is abstract makes it easier to decipher for those who are not necessarily information technology or system dynamics experts. Also, the CMU CERT technical staff focused on describing the balancing and reinforcing feedback loops as they found those to be of utmost interest to business managers (Cappelli and Moore, 2008).

To ensure that all the variables were incorporated, the Insider Threat Logical Data Model and the Insider Threat System Dynamics Model were compared with the Abstracted Common Model. Three areas of focus in this research's models were not completely addressed and were therefore incorporated. The resulting model, the Insider Threat Model for Sabotage and Espionage Model, was then used during the policy review.

3.5 Modification of the Abstracted Common Model

The three areas of the insider threat problem that were covered in this research's models but not, or not fully, in the Abstracted Common Model were motivations, organizational priorities, and social networks. The incorporation of these variables into this research's Insider Threat Model for Sabotage and Espionage (see Figure 22) is explained in the next sections. The importance of these factors in the insider threat problem is explained, as well as their specific relevance to the USAF. These variables were integrated to enhance the comprehensiveness of the policy review.

3.5.1 Insider Motivations

While the Abstracted Common Model does not include an *Insider Motivation* variable, its variable *Personal Needs* (highlighted in yellow in Figure 22) embodies this factor of the insider threat problem. The paper "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," (Band et al., 2006) from which the Abstracted Common Model comes, has some discussion about this connection of motivations to needs, but there can be a more robust relationship explained between these two, using Casey's (2004) six types of motives.

- *Power reassurance* is the need to boost one's self-confidence. For example, the insiders may feel the need to prove to themselves that they can successfully accomplish the act at hand (Mills et al., 2009).
- *Power assertive* is the need for recognition, usually to boost one's self-worth (Shaw et al., 1998).
- *Anger retaliatory* is the need for revenge (Mills et al., 2009).

- *Anger excitation* is the need to gain pleasure from causing harm to the organization and its members (Mills et al., 2009).
- *Opportunistic* is the need to achieve satisfaction (Mills et al., 2009).
- *Profit* is the need for money (Shaw et al., 1998).

In order to detect which insiders may potentially be malicious, it is important for an organization to comprehend why they would decide to attack. The USAF conducts background investigations on its employees to determine their security clearance level. An investigator discovering an individual has financial problems is a concern as it could indicate this individual is susceptible to adversaries approaching him to commit espionage (Under Secretary for Management, 2006). Additionally, the USAF recently went through a period of reductions in force. There are many documented cases of terminated employees becoming disgruntled and plotting revenge on their organizations (McMillan, 2009). If stressful or unfavorable events occur, it is important to understand how they can affect a person's motivation and likelihood to attack.

3.5.2 Organizational Priorities

Another concept that was not included in the Abstracted Common Model was that of organizational priorities and how they affect organizational controls and spending (Rich et al., 2005). An organization that highly prioritizes profits may be less likely to invest money into information technology security. Often this results from the fact that the return on investment with preventive measures can be extremely hard to calculate. An organization may not even know whether an implemented measure is deterring

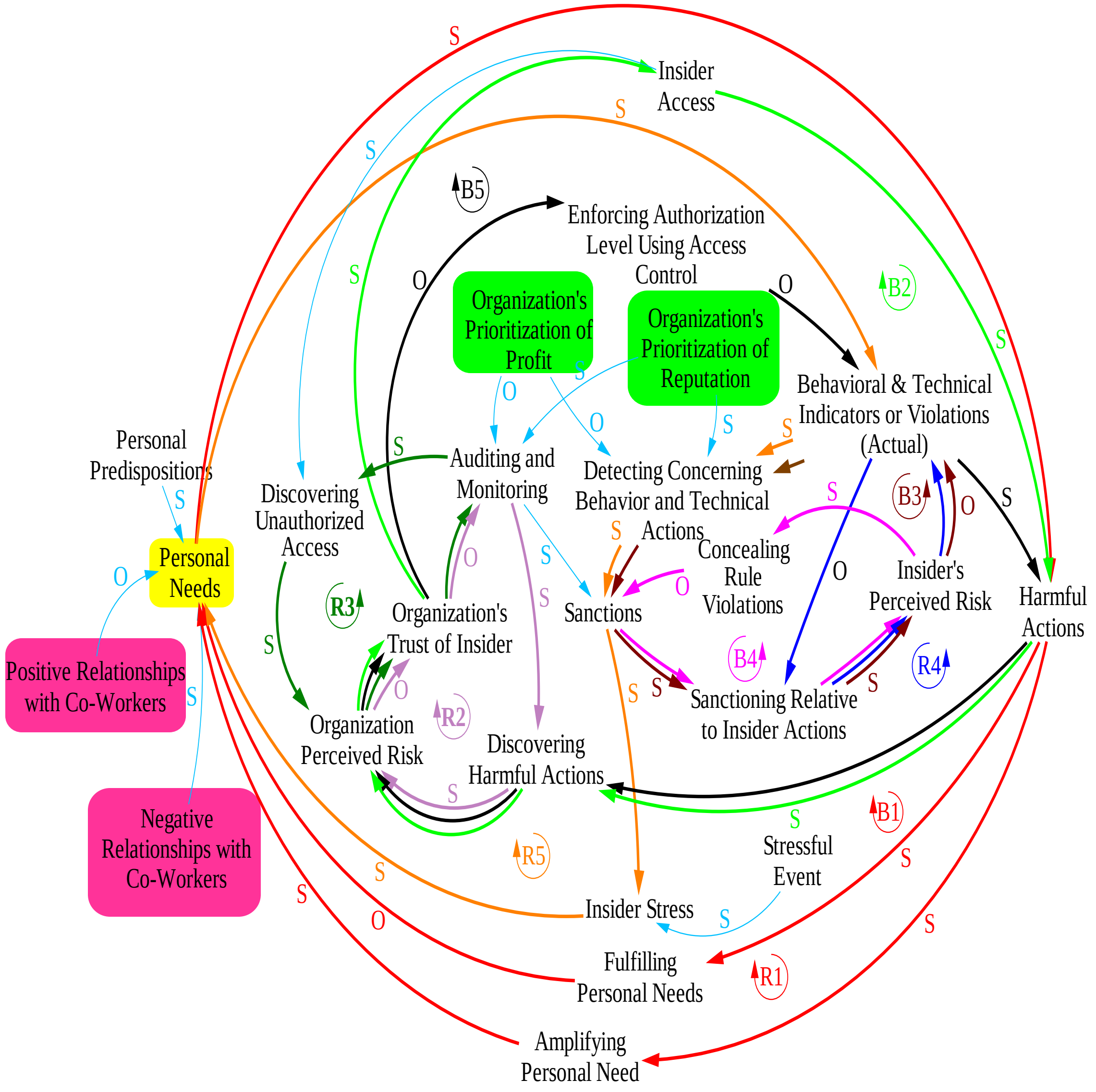

Insider Access
B5
Enforcing Authorization Level Using Access Control
B2
Organization's Prioritization of Profit
Organization's Prioritization of Reputation
Behavioral & Technical Indicators or Violations (Actual)
Personal Predispositions
Discovering Unauthorized Access
Auditing and Monitoring
Detecting Concerning Behavior and Technical Actions
B3
Personal Needs
Concealing Rule Violations
Insider's Perceived Risk
Harmful Actions
R3
Organization's Trust of Insider
Sanctions
Positive Relationships with Co-Workers
B4
Sanctioning Relative to Insider Actions
R4
R2
Organization Perceived Risk
Discovering Harmful Actions
Negative Relationships with Co-Workers
B1
Stressful Event
R5
Insider Stress
Fulfilling Personal Needs
R1
Amplifying Personal Need

Figure 22. Insider Threat Model for Sabotage and Espionage

attacks. On the other hand, a company who highly values its reputation may be more inclined to invest in security measures, as it cannot afford a publicized security breach (Rich et al., 2005). By incorporating these variables into the model, an organization can assess how its stance on profits versus reputation can affect its likelihood of detecting, deterring, and preventing malicious attacks. It is also important to note that insiders are usually privy to the company's stance on security and know how wise it is to attempt an attack.

This issue of prioritization is a difficult one of the USAF. As a responsible steward of its Congressional budget the USAF must make wise investments in security measures. On the other hand, the USAF is responsible for protecting vital information and information systems related to national security and therefore aims for robust security. Determining the appropriate balance is a challenge and can have affects on mitigating threats from malicious insiders.

To incorporate these concepts into the Insider Threat Model for Sabotage and Espionage two additional variables were created (highlighted in green in Figure 22). The variable *Organization's Prioritization of Profit* is negatively correlated with *Auditing and Monitoring* given that an organization which prioritizes profits does not invest as much in monitoring and auditing its employees. This results in fewer harmful actions being discovered. It also does not spend as much money in training its employees which can lead to employees not discovering unusual or malicious behavioral or technical incidents. Therefore, it is also negatively correlated with the variable and *Detecting Concerning Behavior and Technical Actions*. The second new variable *Organization's Prioritization of Reputation* will be positively correlated with both *Auditing and Monitoring* and *Detecting Concerning Behavior and Technical Actions* as this type of organization is willing to invest the money in training, monitoring, and auditing, which increases its likelihood of detecting behavioral and technical precursors.

3.5.3 Social Networks

Though the CMU CERT technical staff members are looking to integrate social networks into future models, they have not yet (Cappelli and Moore, 2008). As discussed earlier, insiders can be affected either negatively or positively by relationships with their co-workers. Having relationships with upstanding co-workers may deter insiders from doing harm to the organization as they do not wish to risk these relationships, either by their co-workers' disapproving of their actions or the company firing them. This is due to the Social Bond Theory (Theoharidou et al., 2005). For example, past research has shown a strong negative correlation between co-worker satisfaction and unexcused absenteeism. The researcher theorized that the employees did not want to jeopardize the professional relationships they had made by exhibiting deviant behavior (Blau, 1985). Additionally, insiders with strong ties within the organization may not want to bring harm to their co-workers in terms of loss in revenue, unrenewed contracts, and tarnished reputation, which can all result from a successful attack (Theoharidou et al., 2005).

Strong relationship ties in the workplace have been shown to have other positive effects, like a sense of community, better communication, and enhanced understanding of the mission of other areas of the organization. The "Rule of 150" describes the supported theory that organizational units with more than 150 members are too large to benefit from many of these positive effects of social networks as the relationships do not develop. In large organizations, employees can feel insignificant and not part of a cohesive team (Gladwell, 2002).

By examining the two case studies discussed in this research, it is evident that neither Robert Hanssen nor Timothy Lloyd had strong social ties that they were concerned about breaking. Hanssen was an introvert with poor social skills (Cooper and Garvey, 2001). He did not relate well with co-workers; there are reports of him sexually harassing and physically assaulting FBI co-workers (Havill, 2001a; Havill, 2001b). He also reprimanded their social behavior and hacked into their computers just for enjoyment (Havill, 2001b). During the end of his time with Omega, Lloyd lashed out at and tried to sabotage co-workers (Melara et al., 2003).

Per the Social Learning Theory, having relationships with co-workers who themselves are committing malicious acts or planning to do so may actually increase the insiders' likelihood of participating in deviant behavior (Theoharidou et al., 2005). The insiders may look at these other individuals as role models or people they wish to impress. The likelihood of such an individual following suit is increased if these deviant co-workers are not being detected or disciplined.

As organizations are designed or restructured, the effects of social networks is important to keep in mind for various reasons, from morale to performance. The USAF strongly promotes teamwork within its organizations which could benefit the USAF in terms of the insider threat problem. There is a concern though regarding how frequently active duty members change units and even bases. It is important to ensure they become part of the team when arriving at a new workplace.

These two concepts are incorporated into the Insider Threat Model for Sabotage and Espionage (highlighted in magenta in Figure 22) by including two variables, each of which has an effect on *Personal Needs*. The first new variable *Positive Relationships with Co-Workers* has a negative correlation with *Personal Needs*, given that those healthy relationships should decrease insiders' need or desire to commit harmful actions. The second variable *Negative Relationships with Co-Workers* should have positive correlations with *Personal Needs,* given that those unhealthy relationships should increase insiders' need or desire to commit harmful actions.

3.6 Summary

This chapter presented this research's Insider Threat Logical Data Model and Insider Threat System Dynamics Model, to include the models' entities, attributes, relationships, and feedback loops. This chapter also explained the selection of the Abstracted Common Model and the additions made to it, resulting in the Insider Threat Model for Sabotage and Espionage, which is used in the USAF policy review.

Chapter IV presents the methodology used for reviewing the DoD and USAF policies in terms of the best practices published by the CMU CERT technical staff and the Insider Threat Model for Sabotage and Espionage. The results of the policy review are discussed, including which practices and variables were addressed, which were not covered, and which were in conflict with the policies. The chapter then presents recommendations that could help the USAF to address the shortfalls and conflicts. Lastly the chapter proposes three new best practices that can be used by any organization.

IV. Policy Review

4.1 Overview

This chapter discusses the methodology used to review the DoD and USAF policies, both in terms of the best practices published by the CMU CERT technical staff this research's Insider Threat Model for Sabotage and Espionage. For each best practice or model variable, this research shows to what degree the policies covered it, to include actors, tools, and areas of focus, such as specific systems, types of insiders, or activities. Additionally, there is a discussion of the shortfalls and conflicts identified in the policies. This chapter presents recommendations aimed to assist the USAF in better mitigating the insider problem. Lastly the chapter offers three new best practices that can be adopted by any organization. While this chapter summaries the findings, a more detailed breakdown is included in Appendix A.

4.2 Methodology of the Policy Review

After the completion of this research's Insider Threat Model for Sabotage and Espionage, the methodology for the review of the DoD and USAF policies needed to be designed. For this review, a pure naturalistic-qualitative strategy was used, from Patton's 2002 "Integrated Model of Measurement, Design, and Analysis" (Trochim and Donnelly, 2007). This strategy began with a naturalistic inquiry; in this case, "Based on its written policies, how well postured is the Air Force to mitigate insider threats?" The next step was to collect qualitative data (Trochim and Donnelly, 2007). Currently, there are hundreds of DoD and USAF policies; therefore, this research looked at a sampling that relate to information assurance (IA) and security, network operations, personnel security, and special investigations. The sample size grew during the analysis phase as selected policies referenced to others which, after being evaluated, were added to the sample.

The sample consists primarily of USAF documents, including Air Force Instructions (AFI), Manuals (AFMAN), and Policy Directives (AFPD). Three DoD-level documents were also analyzed as they are fundamental publications, often the foundation for the policies developed by the individual military branches, to include the USAF. Additionally, the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" were reviewed. These guidelines are approved by the President of the United States and used by all government agencies; the USAF does not have its own set.

The reviewed documents are listed below, grouped into the following four categories: IA and security, network operations, personnel security, and special investigations. For each category, the observables to which they relate are listed and highlighted in the "Cyber Event/Observable Taxonomy" (repeated in Figure 23 for the reader's convenience).

- *IA and Security (highlighted in yellow)*
    - Observables: physical access, materials transfer to handlers, reconnaissance, other actions, exfiltration, communication (cyber), manipulation, counter detection
    - DoD 8500.01E: Information Assurance (IA) (Department of Defense, 2002)
    - DoD 8500.02: Information Assurance (IA) Implementation (Department of Defense, 2003)

  - DoD 8570.01-M: Information Assurance Workforce Improvement Program (Department of Defense, 2005)
  - AFI 31-401: Information Security Program Management (Department of the Air Force, 2005a)
  - AFI 33-204: Information Assurance (IA) Awareness Program (Department of the Air Force, 2004c)
  - AFI 33-230: Information Assurance Assessment and Assistance Program (Department of the Air Force, 2004d)
  - AFMAN 33-223: Identification and Authentication (Department of the Air Force, 2005c)
  - AFPD 33-1: Information Resource Management (Department of the Air Force, 2006c)
  - AFPD 33-2: Information Assurance (IA) Program (Department of the Air Force, 2007)
  - AFPD 33-3: Information Management (Department of the Air Force, 2006d)
- *Network Operations (highlighted in green)*
  - Observables: violations, physical access, reconnaissance, other actions, entrenchment, exfiltration, communication (cyber), manipulation, counter detection
  - AFI 33-115, Volume 1: Network Operations (Department of the Air Force, 2006a)
  - AFI 33-115, Volume 2: Licensing Network Users and Certifying Network Professionals (Department of the Air Force, 2004a)

  - AFI 33-115, Volume 3: Air Force Network Operations Instructions (Department of the Air Force, 2004b)
  - AFI 33-202, Volume 1: Network and Computer Security (Department of the Air Force, 2006b)
  - AFI 33-207: Computer Security Assistance Program (Department of the Air Force, 1997)
- *Personnel Security (highlighted in magenta)*
  - Observables: polygraph results, communications, failure to report (finance, travel, contacts), counter intelligence, foreign travel, personal conduct, social activity, other actions
  - Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Under Secretary for Management, 2006)
  - AFI 31-501: Personnel Security Program Management (Department of the Air Force, 2005b)
- *Special Investigations (highlighted in blue)*
  - Observables: polygraph results, communications, failure to report (finance, travel, contacts), counter intelligence, foreign travel, personal conduct, social activity, other actions
  - AFI 71-101, Volume 4: Counterintelligence (Department of the Air Force, 2000)
  - AFPD 71-1: Special Investigations (Department of the Air Force, 1999)

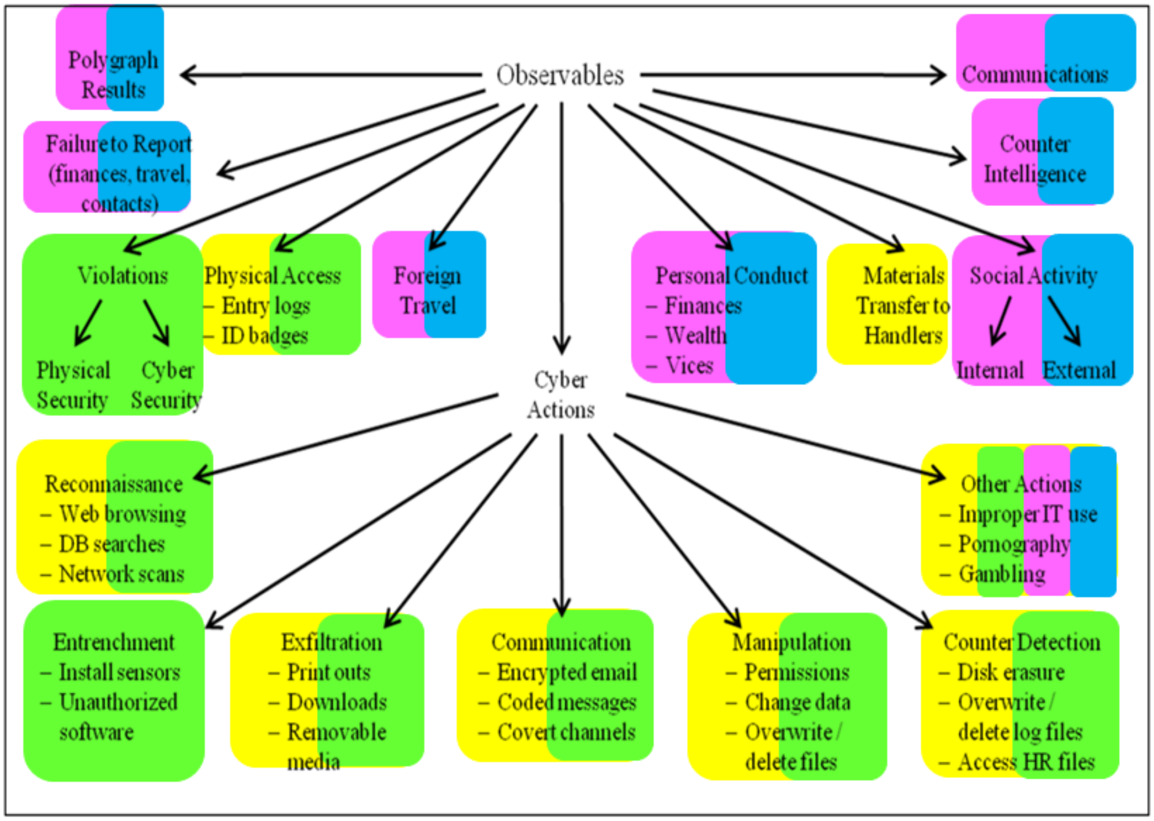

Observables
Polygraph Results
Communications
Failure to Report (finances, travel, contacts)
Counter Intelligence
Violations
Physical Security
Cyber Security
Physical Access
– Entry logs
– ID badges
Foreign Travel
Personal Conduct
– Finances
– Wealth
– Vices
Materials Transfer to Handlers
Social Activity
Internal
External
Cyber Actions
Reconnaissance
– Web browsing
– DB searches
– Network scans
Other Actions
– Improper IT use
– Pornography
– Gambling
Entrenchment
– Install sensors
– Unauthorized software
Exfiltration
– Print outs
– Downloads
– Removable media
Communication
– Encrypted email
– Coded messages
– Covert channels
Manipulation
– Permissions
– Change data
– Overwrite / delete files
Counter Detection
– Disk erasure
– Overwrite / delete log files
– Access HR files

Figure 23. Cyber Event/Observable Taxonomy (Mills et al., 2009)

The next step was to perform a content analysis on these documents. The approach used in this research was a combination of a directed and a summative approach (Hsieh and Shannon, 2005). The directive nature stems from the fact that it was based on the research previously conducted by the CMU CERT technical staff members, to include their Abstracted Common Model and published best practices (described in the next section) (Cappelli et al., 2006). CMU CERT's technical staff provided the overarching concepts which gave necessary direction to the general research question, known as a deductive category application (Mayring, 2000). These works are felt to be trustworthy as the CMU CERT technical staff has been working on the insider threat problem for over six years and has published numerous reports on the subject. Additionally, the staff is sponsored by and has worked with such groups as the United States Secret Service, Defense Advanced Research Projects Agency, Defense Personnel Security Research Center, and many civilian organizations. These works were not produced specifically in regards to or on behalf of the USAF, and it is believed that they not biased towards how the USAF is doing in its fight against insider attacks.

The content analysis also took a summative approach in terms of examining specific key words for each best practice and variable within the Insider Threat Model for Sabotage and Espionage. The analysis, conducted by hand, began with certain key words and phrases with additional words and phrases being added as the analysis progressed. A latent content analysis was conducted as the concern was not simply the word count but the interpretation of the policies which included these key words and phrases. Some policy statements included the key words and phrases but were found to have no relevance to the insider threat problem. Those passages that did relate to this research were recorded and examined to see what insight they provided on the actors involved in implementing the policy, tools used by these individuals, and specific areas of interest, to include particular systems, types of insiders, or activities. For example, section 3.8.1.3. from AFI 33-202, Volume 1 reads,

> Information Protection Operations (IPO) personnel in the NCC will check for antivirus signature files/datfiles updates daily from the AFCERT/DoD CERT sites. Users will pull down new signature files from the NCC-controlled site or NCC's site will replicate (if feasible) new signature files to the users as soon as received. Accomplish a virus scan immediately following an update of a signature file" (Department of the Air Force, 2006b).

This passage has the key word "antivirus" which is linked with best practice number 7, "Actively defend against malicious code" (see next section). After reading this passage, it is clear that it does indeed relate to protecting the USAF network from malicious code, which some malicious insiders use to commit sabotage. IPO personnel are responsible for executing this policy item, and they use the AFCERT and DoD CERT websites and virus scans as tools. There is a focus on using signature-based tools and ensuring signature files are updated daily.

Once all of the policies were individually analyzed, a summary was developed that addressed to what extent each best practice or variable from the model is covered in the policies, to include shortfalls and conflicts. Additionally, overall recommendations were generated to address the areas which need improvement.

4.2.1 Best Practices for Mitigating Insider Threat

After conducting years of research on the insider threat problem and formulating multiple models on the subject, the CMU CERT technical staff has published two versions of the "Common Sense Guide to Prevention and Detection of Insider Threats" (2006). The following list is a compilation of the best practices from the second version of this report and the recommendations for future research made by the CMU CERT technical staff in its comparison of insider sabotage and espionage (Band et al., 2006). As mentioned earlier, each policy document was analyzed to see if it incorporates these best practices. For each one, the analysis looked for the following key words and phrases:

1. *Institute periodic enterprise-wide risk assessments.*

   In order to protect its information resources, an organization must identify possible threats and vulnerabilities, determining both their likelihood and impact. The organization must factor in insiders as potential threat-sources. The organization must balance the costs, to include money and employee morale, against the benefits of enhanced security. Risk assessments can assist it in accomplishing this (Cappelli et al., 2006).

Key words and phrases: controls, countermeasures, critical assets, flaws, impact, likelihood, mitigate, prioritization, risk analysis, risk assessment, risk management, risk mitigation, threat, vulnerability

2. *Institute periodic security awareness training for all employees.*

Management must develop a culture of awareness of insider threats, and an effective way to do this is through training. Employees must understand the policies in place, why it is important that they are enforced, and the repercussions if they are not (Cappelli et al., 2006).

Key words and phrases: awareness, certification, education, espionage, IA, insider threat, licensing, objectives, orientation, sabotage, social engineering, training

3. *Enforce separation of duties and least privilege.*

If the responsibility for essential functions is distributed amongst many employees, the power of a single individual is reduced. In this situation, it would be more difficult for an employee to execute a successful incident of espionage or sabotage without the assistance of others. The security policy of least privilege is also important as it gives employees access only to the resources they need to successfully complete their duties (Cappelli et al., 2006).

Key words and phrases: least privilege, need-to-know, privileged access, role-based access, separation of duty, separation of function, two-person compliance

4. *Implement strict password and account management policies and practices.*

This is one of the most basic preventive measures; it is absolutely essential to ensure authentication and non-repudiation. If insiders are restricted from certain functions due to the policy of least privilege but can compromise other employees' accounts, they can still launch attacks (Cappelli et al., 2006).

Key words and phrases: account review, accountability, authentication, backdoors, biometrics, common access card (CAC), identification, login, network user licensing, non-repudiation, passwords, public key encryption, social engineering, user account, user privilege

5. *Log, monitor, and audit employee online actions. Collect and save data for use in investigations.*

By implementing this measure, an organization may be able to identify technical precursors which are warning signs of a future attack. If noticed in time and dealt with appropriately, the organization may be able to prevent a damaging attack. These logs of employee activity should be maintained in case they are needed as evidence in an investigation (Cappelli et al., 2006).

Key words and phrases: audit, bypass, cataloging, consent to monitoring, file modifications, firewall, log, monitor, network traffic, privilege change, traffic analysis, unauthorized transmissions, VPN

6. *Use extra caution with system administrators and privileged users.*

    These administrators and privileged users hold a lot of power as they are typically the employees who set or implement the policies, as well as monitor the network resources. They can be in the best position to access information or deploy an attack, as well as cover up their tracks (Cappelli et al., 2006).

    Key words and phrases: backup operators, privileged access, privileged user, security manager, system administrators

7. *Actively defend against malicious code.*

    Many sabotage attacks involve the deployment of malicious code such as logic bombs. Though there is no tool that perfectly detects these, security measures should be in place to try to do so, such as looking for the signatures of known viruses (Cappelli et al., 2006).

    Key words and phrases: anomaly, antivirus, baseline, hash function, malicious code, malicious logic, signature, Trojan horse**,** viruses, worm

8. *Use layered defense against remote attacks.*

    Many attackers have been more comfortable executing their malicious actions from a remote location, away from the eyes of co-workers and managers. Therefore security measures and policies regarding remote access must be sound and well executed (Cappelli et al., 2006).

    Key words and phrases: demilitarized zones, proxy, remote access, remote dial-in/dial-out communications, VPN

9. *Monitor and respond to suspicious or disruptive behavior.*

Mitigating insider threat requires a team effort. All members of the organization should be watchful of unusual behavior of their co-workers, and there should be procedures in place allowing them to report anything suspicious. In particular, supervisors need training in this area (Cappelli et al., 2006).

Key words and phrases: acting out of character, alarming statements, alcohol, Article 15, bankruptcy, behavior, counseling, courts-martial, criminal activity, drug, embezzlement, espionage, financial irresponsibility, foreign intelligence, foreign travel, gambling, IA security event/incident, indebtedness, letters of reprimand, mental health, misuse of government property, network security event/incident, report, reportable information, sabotage, stress, spy, suspicious activities, terrorism, theft, treason, unauthorized access, unauthorized release, unauthorized technology transfer, unfavorable information, Uniform Code of Military Justice (UCMJ), work performance

10. *Deactivate computer access following termination.*

The organization should have strict procedures in place to disable all access paths of employees who have been terminated. The lack of such procedures has been detrimental to organizations in the past (Cappelli et al., 2006).

Key words and phrases: departure, deleting user accounts/passwords, disabling user account/password, retire, separation, termination

11. *Implement secure backup and recovery processes.*

In the event of a successful attack, an organization may be able to lessen the negative impact by having backup copies of its information (Cappelli et al., 2006). Management should examine the procedures for creating and maintaining backup materials as an insider, such as Timothy Lloyd, may increase the impact of his attack by reducing the existence of or stealing the backup resources (Melara et al., 2003).

Key words and phrases: backup, contingency, continuity of operations, disaster, ghost image, recovery, redundancy

12. *Analyze current access control policies and practices; identify and evaluate options to mitigate insider threat risk.*

Both physical and electronic access paths must be identified, monitored, and tightly controlled by management (Band et al., 2006). Malicious insiders have often used access paths that are unknown to the organization to commit their attacks.

Key words and phrases: access, Access Control List (ACL), authentication, backdoor, classification, classified information/media/product, clearance, control, IA awareness/training, identification, investigation, licensing, need-to-know, privilege, qualification, remote access, SIPRNET, unauthorized connection

13. *Clearly Document Insider Threat Controls*

Organizations should document all insider threat controls, make sure employees understand these controls, and address violations of such controls

(Cappelli et al., 2006). Controls are not enforceable if employees are not made aware of them (Pipkin, 2000).

Key words and phrases: insider threat control, insider threat countermeasures

4.2.2 Variables of the Insider Threat Model for Sabotage and Espionage

Each document from Section 4.2 was also examined to see if it addresses the variables from the Insider Threat Model for Sabotage and Espionage. Below is the list of the variables as well as whether they are addressed by one of the CMU CERT technical staff's best practices. If they are not, this research specifically analyzed if and how the USAF policies address them. For each of the following variables, any additional key words or phrases not mentioned above are listed:

- *Auditing and Monitoring:* addressed by best practice number 5, "Log, monitor, and audit employee online actions."
- *Discovering Unauthorized Access*: addressed by best practice number 12, "Analyze current access control policies and practices; identify and evaluate options to mitigate insider threat risk."
- *Discovering Harmful Actions*: addressed by best practice number 5, "Log, monitor, and audit employee online actions."
- *Detecting Concerning Behavior and Technical Actions*: addressed by the following best practices:
    - Number 5, "Log, monitor, and audit employee online actions."
    - Number 9, "Monitor and respond to suspicious or disruptive behavior."

  - This research also looks at how USAF policies detect prior concerning behavior through the use of the “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.”
- *Sanctions*
  - Sanctions due to employee behavior are addressed by best practice number 9, “Monitor and respond to suspicious or disruptive behavior.”
  - While best practice number 2, “Institute periodic security awareness training for all employees,” addresses informing employees of the repercussions of violating security measures, it does not address issuing of sanctions. This research also looks at whether USAF policies mandate that supervisors or commanders issue sanctions to employees for inappropriate technical acts.
  - Key words and phrases: access, employee intervention, loss of clearance, network license, Security Information File (SIF), suspension
- *Enforcing Authorization Level Using Access Control* : addressed by best practices
  - Number 3,” Enforce separation of duties and least privilege.”
  - Number 4, “Implement strict password and account management policies and practices.”
  - Number 6, “Use extra caution with system administrators and privileged users.”
  - Number 8, “Use layered defense against remote attacks.”
  - Number 10, “Deactivate computer access following termination.”
  - Number 12, “Analyze current access control policies and practices; identify and evaluate options to mitigate insider threat risk.”

- *Insider Access*- this variable is strongly related to the previous one, and therefore is addressed by the same best practices listed on the previous page
- *Organization's Prioritization of Profit*
    - Not addressed by the best practices
    - Key words and phrases: prioritization, priority, profit
- *Organization's Prioritization of Reputation*
    - Not addressed by the best practices
    - Key words and phrases: prioritization, priority, reputation
- *Organization's Trust of Insider*
    - Addressed in part by best practice number 1, "Institute periodic enterprise-wide risk assessments."
    - This research also looks for any other determinants of trust
    - Key words and phrases: ability, benevolence, integrity, trust, trustworthiness
- *Organization Perceived Risk*: addresses by best practice number 1, "Institute periodic enterprise-wide risk assessments."
- *Insider Stress*
    - Addressed in part by best practice number 9, "Monitor and respond to suspicious or disruptive behavior."
    - This research also looks for any policies that examination employee stress
- *Stressful Event*: similar to "Insider Stress"
    - Addressed in part by best practice number 9, "Monitor and respond to suspicious or disruptive behavior."

  - This research also looks for any policies that call for the examination of stressful events in the employee’s life
  - Key words and phrases: stressful event
- *Personal Predispositions*
  - Not addressed by the best practices
  - While predispositions may be difficult for an organization to identify, this research looks at any policies or procedures that try to glean insight into the employee’s psychological state, perhaps through talking with friends, family, and co-workers
  - Key words and phrases: Many of the same words as for best practice number 9, “Monitor and respond to suspicious or disruptive behavior.” Yet in this case, the behavior or activity occurred in the past, usually identified during a background investigation via the “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.”
    - Others: addiction, allegiance to the United States, dishonesty, disloyalty, dual citizenship, egotism, emotional condition, employment/service to foreign organization, irresponsibility, lack of candor, lack of sound judgment, malicious, mental condition, physical condition, resistant to change, sexual behavior, sexual deviance, social skills, unexplained affluence, unreliability, untrustworthy, violent behavior
- *Negative Relationships with Co-Workers*
  - Not addressed by the best practices

  - Key words and phrases: association, friendship, relationship, social influence, social network
- *Positive Relationships with Co-Workers*
  - Not addressed by the best practices
  - Key words and phrases: same as above
- *Personal Needs*: similar to Personal Predispositions
  - Not addressed by the best practices
  - While needs may be difficult for an organization to identify, this research looks at any policies or procedures that try to glean insight into this, perhaps through talking with friends, family, and co-workers
  - Key words and phrases: bankruptcy, business/financial/property interest in foreign country, disgruntlement, embezzlement, espionage, expectation, financial irresponsibility, foreign influence, gambling, indebtedness, recognition, revenge, sadistic, satisfaction, treason, unexplained affluence

4.3 Findings for Best Practices and Variables

For each best practice or variable, this research discusses to what degree the policies implement it, as well as if there are any aspects that are not covered or any conflicts between the best practice or variable and the policies. Table 1 provides an overarching summary for each as well.

Table 1. Summary of Findings

Best Practice or Model Variable	Overarching Summary
“Institute periodic enterprise-wide risk assessments”	- Too much focus on threats and vulnerabilities, which is only part of the assessment process - Need to evaluate likelihood, impact, and controls
“Institute periodic security awareness training for all employees”	- Many requirements for IA training but very little mention of insider threat - No reference to training employees on detecting suspicious behavior
“Enforce separation of duties and least privilege”	- Widespread mandate for “need-to-know” - Only a few specific examples of separation of duties (all technical)
“Implement strict password and account management policies and practices”	- Strong policies regarding authentication and identification - Fake accounts (“back doors”) not addressed
“Log, monitor, and audit employee online actions. Collect and save data for use in investigations”	- Activities are mandated but lack of guidance on retention and activities for which to look - Time-consuming nature leads to it not being accomplished
“Use extra caution with system administrators and privileged users”	- Call for increased monitoring and visibility of privileged, fairly vague - No separation of duty requirements
“Actively defend against malicious code”	- Discuss signature based tools - No mention of anomaly-based
“Use layered defense against remote attacks”	- Privileged actions are discouraged - Approval authority is unclear
“Monitor and respond to suspicious or disruptive behavior”	Does not include acting out of character, one-time incidents, poor job performance
“Deactivate computer access following termination”	- Policy is general - Unclear regarding who ensures this occurs
“Implement secure backup and recovery processes”	No guidance on what needs to be included (e.g., redundancy, ghost images)
“Analyze current access control policies and practices; identify and evaluate options to mitigate insider threat risk”	Further guidance needed regarding fake accounts, ACLs, system administrators, remote access
“Clearly document insider threat controls”	Few explicit references

“Sanctions” (for inappropriate technical acts)	- Use SIF, suspension or loss of clearance, restriction of access - No mention of employee intervention
“Organization's Prioritization of Profit”	Not discussed
“Organization's Prioritization of Reputation”	Not discussed
“Organization's Trust of Insider”	Addressed in background investigation
“Insider Stress”	Not discussed
“Stressful Event”	Not discussed
“Personal Predispositions”	- Focus on conduct and behavior - Insight into personality not addressed
“Negative Relationships with Co-Workers”	- Discuss associations with persons committing criminal activity and sabotage - No discussion of parties involved in malicious technical activity
“Positive Relationships with Co-Workers”	Not discussed
“Personal Needs”	- Address finances and foreign influence - No discussion of revenge, recognition, self-confidence
“Detecting Concerning Behavior and Technical Actions”	- Focus on mishandling of information - No discussion of suspicious behaviors

4.3.1 Best Practice- “Institute periodic enterprise-wide risk assessments”

The policies talk about identifying threats, vulnerabilities, controls, and risks, and they mandate the execution of risk assessments at all levels from the DoD Chief Information Officer (CIO) to personnel in the network control centers (NCC) to the information system security officer (ISSO) responsible for individual information systems. The policies also establish a hierarchical structure that supports a strong communication flow of security information, to include new vulnerabilities and appropriate countermeasures. Each level receives guidance from higher levels as well as reports to those levels of any security flaws or suspicious network behavior.

Other actors who play a role in executing this best practice include the following: Defense Information Systems Network Designated Approving Authority (DISN DAA), AF Communications Agency (AFCA), 92d Information Warfare Aggressor Squadron (92 IWAS), AF Network Operations and Security Center (AFNOSC), and IA offices at the Major Command (MAJCOM), Numbered Air Force (NAF) and base levels. These actors use many tools to complete the risk assessments to include information from the DoD CIO Annual IA Report, DoD uniform risk criteria, Information Assurance Vulnerability Alerts (IAVA) and bulletins (IAVB), and AF Office of Special Investigations (AFOSI). They identify potential risks through the adjudicative process, independent audits (to include Scope EDGE and 92 IWAS red teams), self-assessments, and certification and accreditation (C&A) process. NCCs and ISSOs also utilize Vulnerability Assessment Tools, network vulnerability or penetration testing, and IA security incidents and patterns from network logs and scans. The areas of focus addressed in the policies were systems at all levels (DoD, service, and base), interconnected systems, enclaves, wireless networks, port management, software patches, biometrics, directives and technical orders, system life-cycle documents, continuity of operations plans (CONOPS), and training and awareness programs.

Though there is much discussion of identifying threats, vulnerabilities, and controls, there is little or no discussion regarding two vital steps in a risk assessment: likelihood determination and impact analysis. AFI 33-115, Volume 1 does require AFNOSC, NOSCs, and NCCs to measure the impact of incidents that *have occurred*, but there is no discussion of these employees estimating the effects of an attack that *could occur* (Department of the Air Force, 2006a). AFPD 33-2 was the only policy to mention that security measures invested into an information system should be “commensurate with the shared risk and potential harm that could result from disclosure, loss, misuse, alteration, or destruction of the information" (Department of the Air Force, 2007). There are no policies regarding estimating the likelihood of a security incident. Risk cannot truly be determined without a complete identification of likelihood and impact.

4.3.2 Best Practice- "Institute periodic security awareness training for all employees"

The policies clearly address the goals of the DoD and USAF to ensure all employees receive both initial and annual refresher IA training. There is also discussion of providing an increased depth for students who may become involved in planning, programming, managing, operating, or maintaining information systems. Lead actors include the DoD CIO, Air Education and Training Command (AETC), United States Air Force Academy, AFCA, IA offices, unit commanders, unit IA awareness managers, and the end users (to include military, civilian, guard, reserve, government contractors, and foreign national employees). These actors use initial military training, Air University courses, civilian career programs, the "Air Force Information Assurance Awareness Training" computer-based training (CBT), the USAF IA Home Page (https://private.afca.af.mil/ip), the DoD CIO Annual IA Report, Counterintelligence Awareness Briefings, pamphlets, posters, screen savers, and videotapes in order to teach personnel IA concepts, measures, and tactics.

The major areas of focus for these training programs and materials are as follows: authorized and proper use of information systems and the Internet; account and password policies; threats, vulnerabilities, and countermeasures; privacy rights and consent to monitoring; responsibilities of responding to and reporting suspicious activities and conditions (e.g., social engineering and threats from foreign entities); and duty to protect information systems.

While the concepts listed above factor into the insider threat problem, there are few specific references to insider threat. DoD 8570.01-M does require IA training to include "examples of internal threats such as malicious or incompetent authorized users, users in the employ of terrorist groups or foreign countries, disgruntled employees or Service members, hackers, crackers, and self-inflicted intentional or unintentional damage" (Department of Defense, 2005). Despite this DoD mandate, only two USAF policies were found to explicitly address insider threats. AFPD 33-2 calls for awareness briefings on "insider threat" from AFOSI (Department of the Air Force, 2007), and AFI 33-204 states that one goal of IA awareness if for users to understand countermeasures to protect against sabotage and espionage (Department of the Air Force, 2004c). In addition, DoD 8570.01-M specifically requires teaching users about social engineering risks, but this is the only document to mention social engineering; no USAF documents refer to it. Furthermore, there is no discussion regarding malicious insiders employing social engineering tactics which the CMU CERT technical staff discusses in its "Common Sense Guide to Prevention and Detection of Insider Threats" (Cappelli et al., 2006).

Another shortfall is the quality of training. DoD 8570.01-M calls for IA training to be

> …current, engaging, and relevant to the target audience to enhance its effectiveness. Its primary purpose is to influence behavior. The focus must be on actions that empower the user to mitigate threats and vulnerabilities to DoD systems. Authorized users must understand that

> they are a critical link in their organization's overall IA posture (Department of Defense, 2005).

The USAF's main method for training is the IA CBT, but research has shown that training which involves face-to-face interaction is more successful, both in terms of effectiveness and satisfaction (Heinze, 2004). While a study by Piccoli et al. (2001) did not find a decrease in training effectiveness within a virtual environment, the study's participants did feel a significant shift of responsibility from the instructor to themselves and had problems adjusting to the learning environment. DoD 8570.01-M recognizes that the user is essential in achieving a secure environment but may not be effectively sending this message through the current training program (Department of Defense, 2005). To mitigate insider threat it is indeed essential to gain the help of all employees, but the policies are not emphasizing the requirement to teach them about insider threat. Users are given the responsibility to report suspicious behaviors, but they are not provided with examples of malicious insider behavior might look like. Additionally, some of the methods mentioned are not widely known about or used, to include the USAF IA Home Page and AFOSI briefings.

4.3.3 Best Practice- "Enforce separation of duties and least privilege"

The DoD and USAF offer strict guidelines about limiting information access. Holding a security clearance does not entitle an individual to all information at that level of classification; there also must be a valid work-related reason, or *need-to-know*. The policies do focus on the security and protection of classified information, as well as military intelligence, proprietary information, and web sites containing official information. There is also much oversight of access to privileged programs, utilities, and files, such as system parameter and configuration files, databases, assemblers, debuggers, password files, and activity logs. Special attention is paid to the access granted to joint and coalition partners and those only working within a unit for a short amount of time. The main actors in implementing these policies include the AFNOSC, NOSCs, Top Secret Control Offices, IA personnel, system administrators, and all authorized users.

While there were a few areas that require separation of duties or two-person compliance (Time Compliance Network Orders [TCNO], Top Secret Control Accounts, and IA functions) they were all specifically related to information or information systems. Besides TCNOs, there are no policies regarding NOSC and NCC functions establishing separation of duties. It can be dangerous not to have checks and balances in place within the administration of the network and its vital systems. Additionally, managerial, administrative, and personnel responsibilities should also be compliant with these security policies. If one employee has too much power and is not being monitored, s/he may be able to cause harm and not even be detected.

4.3.4 Best Practice- "Implement strict password and account management policies and practices"

The policies regarding password and account management cover two of the most important issues, accountability and non-repudiation. In order to identify and possibly prosecute a malicious insider, an organization needs to be able to prove that the insider was indeed the executor of the attack. Non-repudiation means that someone cannot deny or refute an action they have performed. The CAC has been implemented throughout the DoD as a method to provide improved network security and non-repudiation via digital signatures. If an individual commits an attack using his network account while using a CAC and personal identification number (PIN), then it is much more difficult for that person to deny the event. While it is still possible that someone could have stolen the person's CAC and compromised the PIN, it is generally accepted that the CAC/PIN combination provides a much higher level of security than a simple username/password combination.

DoD and USAF policies also implement strong identification and authentication procedures to include strict passwords requirements (when the CAC is not feasible) and biometrics. They also require network security personnel to monitor accounts and actively search for vulnerabilities such as weak passwords. The policies cover such topics as assigning, suspending, and deleting user IDs, passwords, and privileges; resetting passwords; updating e-mail addresses; one-time passwords; dormant accounts; rapid log-on retries; reusable generic or group usernames; remote sessions; and trusted profiles (e.g., system administrator, security officer, root user, super user, and backup operators). Key players in implementing these policies are NOSCs, NCCs, system administrators, unit security manager, client support administrators, and all users. These personnel use tools such as favorable background investigation, the Personnel Security Management Program, proper security clearances, password cracking tools and enforcement software, IA training, and internal and external assessments.

One of the major shortfalls in the DoD and USAF policy is that there is no explicit check for the fake accounts (or "back doors"), which malicious insiders often create to conduct their activities. There are policies regarding granting accounts (to include the requirements for a valid security clearance, background check, and IA training), checking for dormant accounts, and terminating accounts, but in no document reviewed for this research was there a requirement for a comparison of current users and active accounts.

As strong as network policies are in the DoD and USAF, most research shows that the greatest security shortfall is people. Humans are susceptible to being lazy, complacent, forgetful, deceived, or malicious, which can all result in a security incident. For example, if while gone from their office, personnel leave their CACs in their computer and their pins or passwords written on a piece of paper in their desks, malicious insiders can access their accounts. Employees may also give out their passwords to co-workers before leaving for vacation or to a stealthy social engineer. The policies are only as good as the users required to follow and enforce them. Users must understand the vital role they play in information security.

4.3.5 Best Practice- "Log, monitor, and audit employee online actions. Collect and save data for use in investigations"

The reviewed policies cover the monitoring of activities such as logging into and modifying information on individual systems and the network. Special attention is paid to suspicious activities such as changes to access controls, privileges, and passwords; unauthorized transmissions or attempts to bypass security measures; unauthorized installation of modems; attempts to access activity logs; unsuccessful log-in attempts; and attempted or realized penetrations. The policies also focus on protecting the core network services and devices, as well as VPN tunnels; this is important as many insiders launch attacks through VPN connections. Network professionals are required to use these logs to identify weak configurations and security deficiencies. Also all users are to be informed that their activities on government systems are being monitored. Lastly, it is stressed to associate any network incident with the responsible party, to enforce accountability and non-repudiation.

Important actors identified in these policies are system administrators, ISSOs, and computer network defense (CND) personnel. These parties use the following tools: firewalls; log files pertaining to errors, network traffic, and intrusions; and, when possible, automated responses of information systems to abort or suspend unauthorized user activity.

Though all network users are reminded of their consent to monitoring via pop-up messages on their computer screens and in their IA training, there is not much attention paid to what types of activities are monitored. There are also many other work-related activities that could be monitored, such as changes in arrival and departure times, printing or transmitting more files, or accessing files not needed for work. While there is guidance requiring auditing, there is not much description regarding which specific activities to look and how long to retain the log files. Between August 2005 and July 2006, the DoD Inspector General (IG) found information assurance weaknesses due to audit trails during 6 out of 16 of their audits. One finding was that standard procedures were not in place and reviews occurred informally, relying on “infinite permanency in personnel positions and consistent memory” (Department of Defense Office of Inspector General, 2006b). Another issue is that there is not always sufficient time, personnel, and technology to audit logs effectively. Another audit conducted by the DoD IG found that often the auditing of log files did not occur because to do so was “cumbersome and time-consuming” (Department of Defense Office of Inspector General, 2006b).

4.3.6 Best Practice- "Use extra caution with system administrators and privileged users"

The DoD and USAF policies clearly outline the level of investigation needed for personnel in security management and administration jobs, paying particular attention to contractors and foreign nationals. Additionally, AFI 33-202, Volume 1 and AFMAN 33-223 both mandate that system administrators will not have "personal accounts with domain administrative privileges" (Department of the Air Force, 2006b; Department of the Air Force, 2005c). The policies also focus on increased monitoring of users with access to Automated Information Systems and ensuring that security professionals only use i-TRM password cracking tools on the systems for which they have responsibility.

Key actors are IA personnel, specifically managers, as well as the commanders and supervisors in charge of assigning personnel to these privileged positions. In addition to background, local agency, and credit check investigations, these employees use CACs, hardware tokens, training and certification requirements, and Privileged Access Agreements to maintain visibility over these vital roles.

As mentioned earlier, policies do require separation of duty among IA functions but do not state the same for other important security functions like system administration. In addition, the language used in these policies is not very clear. AFI 33-202, Volume 1 calls for the wing IA office to maintain "visibility over all privileged user assignments" (Department of the Air Force, 2006b), and AFI 31-501 calls for "commanders and or supervisors [to] have ensured increased monitoring of the individual having AIS access" (Department of the Air Force, 2005b). Both of these statements do not provide much guidance on the level of monitoring and visibility that is appropriate.

4.3.7 Best Practice- "Actively defend against malicious code"

The policies reviewed for this research discussed many tactics for fighting against malicious viruses which may enter the network from various sources, to include software, e-mail, and websites. Vital actors include AFCA, AFNOSC, NOSCs, NCCs, IPO personnel, CND personnel, DAA, ISSO, CSA, and authorized users. The antivirus tools used by these employees are signature-based meaning that they look for known viruses. IPO personnel are required to check daily for new signature files from DoD and USAF Computer Emergency Response Team websites.

Other areas of focus include wireless networks, freeware, firmware, shareware, public domain software, and removable and fixed media. In addition to antivirus tools, these security personnel fight malicious code with software patches, security fixes, configuration management, malicious logic reports, and user awareness training. One theme within these policies is to protect the systems by limiting the modifications that a typical network user can make to an information system, thereby eliminating the chance of them introducing malicious code to the organization. Similar to the results described earlier, the hierarchical structure of the DoD and USAF is utilized to assist in the defense of malicious code, especially in regards to the latest information flowing down to the NCCs.

While signature-based tools can be very effective at detecting known attacks, they cannot detect modified or new attacks. It is advisable to have anomaly-based tools which detect abnormal events, traffic, or configurations (Grimaila, 2008). These were not discussed in the reviewed policies.

4.3.8 Best Practice- "Use layered defense against remote attacks"

The policies mandate the use of proxy services and demilitarized zones to protect the information resources while allowing remote access for telework. In addition, the execution of privileged actions during a remote session is highly discouraged. IAMs and IAOs are required to maintain and review access and activity logs of all remote sessions, paying close attention to any privileged actions, if they are allowed. The policies also prohibit the call-forwarding capability on modems and call for the disconnection of sessions after 15 minutes of inactivity. The NOSCs and NCCs play the prominent roles in executing and enforcing these policies, and they use such tools as VPN client software, access tables, and screened subnets.

There is no discussion in the policy regarding who the approval authority is for allowing remote access and deciding what functions may be executed remotely. Additionally, there is no explicit policy regarding the termination of remote access; they may be handled like all other network accounts. Organizations need to handle remote access very carefully as malicious insiders often feel more comfortable doing harm from outside the office where they are not physically being monitored (Cappelli et al., 2006).

4.3.9 Best Practice- "Monitor and respond to suspicious or disruptive behavior"

The policies focus on the following types of behaviors: criminal activities, technical incidents, financial problems, and family issues. Examples of concerning behavior are indebtedness, child or spouse abuse, action threatening network security, request for unauthorized access to controlled information, unauthorized technology transfer, and contact with a known or suspected foreign intelligence officer or foreign diplomatic establishment. AFPD 71-1 mandates the AFOSI to conduct counterespionage operations (Department of the Air Force , 1999). The other major actors are the Central Adjudication Facility (CAF), commanders, security officials, NCCs, and IAOs, and they use security information files, investigation reports, and mental health evaluations. In addition, all users are required to report any of these types of behavior that they personally witness.

Some suspicious behaviors identified in insider threat research were not discussed in the policies, to include employees acting out of character or making alarming statements (Puleo, 2006). Additionally, AFI 31-501 states that poor duty performance or a one-time incident related to alcohol or poor judgment should not warrant the creation of an SIF, which is used when determining if employees should retain their security clearance (Department of the Air Force, 2005b). This is not consistent with the guidance from the CMU CERT technical staff.

4.3.10 Best Practice- "Deactivate computer access following termination"

The USAF policies call for the disablement and deletion of user accounts of employees leaving the organization. The NOSCs, NCCs, system administrators, and CSAs work together to make this happen. AFMAN 33-223 states, "Ensure procedures are in place so the Network Control Center, workgroup manager, and system administrator are notified when an employee (military, civilian, or contractor) transfers, retires, separates, or is terminated" (Department of the Air Force, 2005c). The language of this is a bit weak as it does not explicitly assign the responsibility of notifying these entities. In DoDI 8500.2 the responsibility of notifying IA personnel when access to an information system is no longer needed is assigned to "authorized users" (Department of

Defense, 2003). If the responsibility is solely in the hands of the employees, they may not follow this in order to keep their accounts.

4.3.11 Best Practice- "Implement secure backup and recovery processes"

Per the policies, AFNOSC, NOSCs, and NCCs all must have backup, continuity of operation, and recovery plans in place. Additionally, AFNOSC is required to assist NOSCs and NCCs with their plans. The policies mandate network personnel to backup servers daily and test recovery procedures quarterly. What these plans should include is not spelt out in the policies. For example, there is no discussion of whether redundant servers should be in place or whether ghost images should be maintained.

4.3.12 Best Practice- "Analyze current access control policies and practices; identify and evaluate options to mitigate insider threat risk"

The DoD and USAF policies discuss the major topics surrounding access control, to include identification and authentication. Access is further contingent on security clearances and need-to-know for the mission at hand. Additional restrictions for special users, such as foreign nationals, contractors, and volunteers, are identified as well. Particular attention is paid to privileged users, classified or controlled information, SIPRNET systems, remote access, shared files, firewalls, and intrusion prevention systems. The USAF Information Warfare Center and NCCs are required to report all backdoors and unauthorized connections to the NOSCs. Other topics covered are building and area entry controls, granting of interim access, and deletion of access.

AFNOSC, unit commanders, ISSOs, and IAOs also play roles in granting and controlling access to information and information systems. They use such tools as user licensing, position requirements and qualifications, IA awareness and training, network components using media access control, Access Control Lists (ACL), and system security authorization agreements.

Many successful insider attacks have included the creation of dummy accounts and back doors; therefore, access control is of utmost importance (Cappelli et al., 2006). While the reviewed policies do discuss managing ACLs, the only specific regulations are for CND systems, such as firewalls and intrusion prevention systems, and service delivery point routers. Also, as mentioned previously, the procedures for notifying the network personnel that an employee's access should be removed are fairly vague and leave the responsibility to "authorized users."

4.3.13 Best Practice- "Clearly document insider threat controls"

While these results show that the DoD and USAF have controls in place to mitigate insider threat, they are rarely stated as such. The only explicit references are in regards to training employees on insider threat and reporting suspicious behavior related to espionage or sabotage.

4.3.14 Variable- "Sanctions" (for inappropriate technical acts)

In terms of issuing sanctions, the policies focus on the suspension or loss of a security clearance and restricted access to controlled areas or information. The CAF, DAA, commanders, and CSAs are all involved and primarily use information within the SIF and regarding violations of the licensing principles to make their decisions. These principles are spelt out in AFI 33-115, Volume 2 and include "failure to maintain an acceptable level of proficiency on a critical program; actions that threaten the security of a network or a governmental communications system; [and] actions that may result in damage or harm to a network or governmental communications system" (Department of the Air Force, 2004a).

As discussed earlier, sanctions can have varying effects. While for some employees it increases their risk adversity and therefore decreases their motivation to cause further incidents, for others it increases both their disgruntlement and motivation to cause an attack. The CMU CERT technical staff recommends using employee intervention to help reduce the disgruntlement (Cappelli et al., 2007). This organizational control is not discussed in the DoD and USAF policies.

4.3.15 Variable- "Organization's Prioritization of Profit"

Given that the USAF is a government agency, it is not in the business of generating profits, which would naturally lead to the conclusion that it would be willing to invest significantly in security controls. One caveat is that the USAF's funding is approved by Congress and therefore it does not have complete control over how its budget is spent.

4.3.16 Variable- "Organization's Prioritization of Reputation"

Given that the USAF is in the business of national security, it is inherently concerned with its reputation, in the eyes of the citizens of the United States, of its allied nations, and of its adversarial nations. It would make sense to conclude that the USAF would want to invest extensively in security controls. Similar to the section above, the USAF is limited by its Congressional budget.

4.3.17 Variable- "Organization's Trust of Insider"

The DoD and USAF policies discuss the fact that complete confidence cannot be achieved, so a risk management approach is used to determine access to critical information and systems. The "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" are important tools for those in charge of granting access. There guidelines cover all three of the aspects of trust outlined in this research, ability, integrity, and benevolence. In terms of ability, the guidelines look at the individuals' psychological conditions, possible addictions, and any past incidents where they proved their failure to protect controlled information or correctly use information systems. The guidelines relevant to benevolence are concerned about employees' allegiance to the United States, as well as their foreign influence, preference, or activities. In terms of integrity, the guidelines look at the individuals' criminal record, financial activity, and history of use and handling of information and information systems.

4.3.18 Variable- "Insider Stress"

The stress level of insiders can play into their disgruntlement and desire to satisfy their personal needs, perhaps at the detriment of their organization (Band et al., 2006). Supervisors and co-workers should look for displays of stress and intervene to prevent the problem from escalating. The DoD and USAF policies do not discuss this aspect of the insider threat problem.

4.3.19 Variable- "Stressful Event"

The occurrence of a stressful event historically has been a trigger for malicious insider attacks (Band et al., 2006). Similar to the section above, supervisors should be monitoring for such events, whether they are events that affect the entire organization (like a reduction-in-force) or just one employee (like a divorce). The DoD and USAF policies do not discuss this aspect of the insider threat problem.

4.3.20 Variable- "Personal Predispositions"

By conducting background investigations, the DoD and USAF examine an employee's predispositions quite thoroughly, covering areas such as criminal activity, mental health, allegiance to the United States, addictions, sexual behavior, inappropriate handling of information and information systems, and financial responsibility. The investigation also entails obtaining a historical picture of the individual's personal conduct, by talking with employers, co-workers, and family and friends. Areas of interest are disloyalty, dishonesty, unreliability, untrustworthiness, lack of sound judgment, irresponsibility, lack of candor, disruptive or violent behavior, and unwillingness to comply with rules and regulations.

One aspect that is not covered in the policies is trying to obtain insight into an individual's personality, to include whether the person is malicious, egotistical, resistant to change, and lacking in social skills.

4.3.21 Variable- "Negative Relationships with Co-Workers"

The policies focus on relationships an employee has with individuals who have exhibited a weak allegiance to the United States and committed espionage, treason, terrorism, or sedition. Per the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," background investigators also look for an employee's association with persons who have a history of criminal activity or sabotage. The policies do not discuss identifying an employee's relationships with co-workers who have committed technical or behavioral precursory events at work.

4.3.22 Variable- "Positive Relationships with Co-Workers"

Though the DoD and USAF policies did discuss searching for unhealthy relationships, they do not mention researching those which an individual has with favorable co-workers. While the USAF promotes teamwork, the frequency of relocation for active duty employees could affect how socially tied to the organization they are.

4.3.23 Variable- "Personal Needs"

In terms of personal needs the policies cover those related to finances and foreign influences. Per the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," background investigators look for evidence of unexplained affluence, embezzlement, frivolous spending, gambling problems, or inability to live within one's means or repay debts. The investigators also search for "substantial business, financial, or property interest in a foreign country" (Under Secretary for Management, 2006). The policies do not discuss gaining insight into the individuals' need for revenge, for recognition, to prove their talents, or to boost their self-confidence. Additionally, the policies do not instruct investigators to uncover evidence of a sadistic nature.

4.3.24 Variable- "Detecting Concerning Behavior and Technical Actions"

As mentioned earlier, there are policies in place to monitor suspicious behavior in the workplace in terms of technical incidents, to include actions threatening network security, requests for unauthorized access to controlled information, and unauthorized technology transfers. In accordance with the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," background investigators also look for past incidents of mishandling protected information or information systems. Examples of concerning behavior include the following: copying or disclosure of controlled information, storing controlled information in an unauthorized location, noncompliance with procedures or regulations, unauthorized modification or destruction of information systems, and unauthorized introduction of hardware or software.

As mentioned previously, the policies do not include guidance and requirements for detecting behavior precursors such as decrease in job performance or making alarming statements.

4.4 Recommendations for Better Mitigating Insider Threat

This next section presents recommendations for nine areas which were identified in this research as needing additional measures in order to better protect the USAF from insider attacks.

4.4.1 Risk Management and Backup Plans

While risk management is covered significantly in the DoD and USAF policies, the focus is on identifying threats and vulnerabilities. Additionally, the USAF must determine the risk of a threat-source exercising or triggering a vulnerability. The risk is comprised of both the likelihood and impact of this occurring. Organizations must also assess the ability of current controls to mitigate this risk. Determining the risk is important as it guides investments in security controls and the creation of security policies (Stoneburner et al., 2002). Organizations often prioritize high-risk assets as they are more likely to be compromised or the impact would be significant if they were.

The prioritization of assets is an important element in creating sound backup and recovery plans as well. To achieve continuity of operations in the event of an attack, redundancy should be built into the network, especially for high-risk assets. If the attack completely destroys resources, those that are high-impact are often those that an organization wants to replace and put back on line first. The DoD and USAF policies briefly discuss the need for backup and recovery plans, but it is advisable for greater emphasis and detail to be provided, to include the incorporation of risk management.

A key element to the success of an enterprise risk assessment is the involvement of leadership, not simply network professionals. The leaders are best qualified to assess factors such as impact to mission. The leaders also need to be in charge of determining and balancing the organizational priorities. Though the USAF is not a profit-oriented business, it does have to be a responsible steward of it Congressional budget. Since the USAF is highly concerned about its reputation, the prioritization of investments is even more challenging; the USAF must aim for strong security on a tight budget.

4.4.2 Limit Power of a Single Employee

Historically, many successful attacks have resulted from one individual, such as a system administrator, possessing too much power on the network. It is vital to have checks and balances with the organization to prevent this. One such method is to require two-person compliance for privileged activities. While the DoD and USAF policies require this for a select few activities, it is advisable to require it for more. One such activity that would be a prime candidate for two-person compliance is the production of data back-ups. An organization can have sound recovery plans, but if a malicious network professional is purposefully not creating, destroying, or stealing the back-ups, the plans will be of little use. The fact that Timothy Lloyd stole the back-up tapes from the Omega Engineering Corporation greatly increased the damages to the company

(Melara et al., 2003). Another activity for which it is advisable to have two-person compliance is the creation of new user accounts. Many successful insider attacks have included insiders creating bogus accounts in order to commit the malicious acts (Cappelli et al., 2006).

As mentioned earlier, these policies of separation of duties and least privilege should be applied to more than just activities related to information systems. An organization's security can benefit from these being embraced for managerial, administrative, and personnel functions as well.

4.4.3 Account Management

As mentioned in the previous section, account management is a vital aspect of the mitigation of insider threat. In addition to closely monitoring the creation of new accounts, network professionals should frequently check for bogus accounts. This should be done randomly; if it is done on a certain day every month, a malicious user could delete the phony account before it would be detected (Cappelli et al., 2006). ACLs should be monitored consistently and randomly as well. Finally, while the policies require special attention for SA and other privileged accounts, the specifics of this should be outlined, to include the frequency of and what is included in checks. Examples of activities that should be monitored are as follows: creating user accounts, modifying systems or policies, running scripts, and modifying logs (Cappelli et al., 2006).

The accurate deletion of accounts, privileges, and access is also essential in mitigating insider attacks. The DoD and USAF policies mention that procedures should be in place to ensure deletion occurs, and most likely the specific measures are spelt out at a lower level of documentation. In terms of these measures, it is recommended that the user whose access is being deleted is not the one responsible for notifying the network professionals. It would be better to have the supervisor notify the appropriate network personnel. The extended use of the CACs should be helpful as well, as long as procedures are in place for the revocation of them upon termination.

Since malicious insiders have been found to be more comfortable executing inappropriate behavior from remote accounts, such accounts need to be highly monitored (Cappelli et al., 2006). The policies should explicitly state who grants permission for remote access, such as a unit commander. Additionally, while the policies discourage the ability for remote users to execute privileged actions, a more strict and explicit policy may be more effective. It would be best to clearly spell out which functions are of special concern and who would decide whether these could be executed remotely.

4.4.4 Monitoring Online Actions

While the policies clearly require the collection and auditing of activity logs, there should also be specifics regarding for which activities to look, how often logs are reviewed, and how long they should be maintained. Additionally storage space and bandwidth are serious concern for the USAF. Logs can obviously not be kept indefinitely, and the amount of data collected can overwhelm some networks, especially those which are deployed. Research should continue in the area of automated auditing tools, such as the work being done by MITRE (Lee, 2007).

4.4.5 Creating Baselines

Per the reviewed policies, the USAF primarily identifies malicious code through the use of signature-based tools which look for known dangerous code. The USAF could benefit from using anomaly-based tools which look for changes to vital files. Many attacks target such files as “Windows Explorer” and “Task Manager” to cause damage and hide their own presence and activity (Grimaila, 2008). If the USAF was to create and maintain baselines of these files and routinely compare them to the files’ current state, then alterations could be detected.

The USAF could also create baselines of typical user behavior on the network. If users began to act abnormally, such as looking at files they do not usually access or working odd hours, this could trigger the network professionals to look more closely at these users’ activities. Unfortunately, creating and maintaining baselines for all network users would be quite time-consuming and expensive. Given the USAF’s current budget, it might be wise to focus on privileged users such as system administrators. While anomaly-based tools can detect unusual network activity and attacks that do not have signatures, they can also trigger many false positives (Grimaila, 2008). This could lead to network security professionals wasting their time investigating innocuous activity and morale decreasing if employees feel the USAF has little trust in them and is suspicious of anything they do out of the ordinary.

4.4.6 Training and Awareness

Training and awareness regarding insider threat is one of the most important tactics the USAF could adopt. All employees should understand the significance of the threat and what the possible damages are. They should understand what variables and specific behaviors are common among malicious insiders so that they may be better prepared to identify and report them. In the cases of both Robert Hanssen and Timothy Lloyd, there were many behavioral warning signs, but co-workers were either uneducated or reporting procedures were not in place. All USAF employees must understand that they all play a role in the mitigation of insider threat; deterrence and detection is dependent on everyone working together. Often a co-worker dismisses suspicious behavior of a fellow employee because it is a one-time occurrence, and s/he does not want to get the individual into trouble. What the co-worker may not know is that suspicious behavior has also been witnessed by others. The conglomeration of all the incidents is what could signal to an organization that it needs to intervene before an attack occurs.

While the DoD and USAF policies include many insider threat countermeasures, the typical network user may not be aware of them. Given the amount of information available today, it would not be surprising if employees do not read every security policy. Similar to the discussion of auditing log files, some work-related activities are very time-consuming, and subsequently there may not be time for all of them to be accomplished. Insider threat training and awareness should ensure that employees are indeed educated about them (Cappelli et al., 2006). The success of some of these controls relies on the employees' correct implementation of them. For example, the USAF requires CACs for logging onto most information systems. If users are sharing their pins or not locking their work stations when they are away from their desks, this security measure is not effective. While hopefully most employees know not to give their passwords or access to their accounts to outsiders, they must understand the importance of maintaining the same diligence with their co-workers as well. Additionally, potential malicious parties may be less inclined to try to forge an attack if they are aware of all the security measures in place, such as monitoring of online activity (Cappelli et al., 2006).

Training programs should also focus on the tactics that malicious insiders may use against their co-workers. When being made aware of social engineering, USAF employees should be instructed that many malicious insiders use this method to gain necessary information for their attack. Employees cannot only monitor the behavior of those outside the organization; they must be wary of co-workers who are asking for information they do not need or are not authorized to access.

Currently the USAF conducts the majority of its IA training via computer-based training during which an individual user reads text and then answers questions. To improve the benefit and enjoyment of training, it is recommended that the USAF look into more interactive training methods. These could include scenario-based online games or discussion-based workshops. The CMU CERT technical staff has developed case studies for organization to use in training situations which can help employees practice what they are being taught (Moore et al., 2008). Currently, due their sensitive nature red team outbriefs are only presented to top leadership. It is recommended that as much information as possible is also given to the general populace so that they can learn from their own mistakes.

4.4.7 Gaining Insight into Personality of the Insider

While the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" look into an individual's past behaviors, it would also be wise for the investigators to develop a personality profile on the person by talking with their family, friends, co-workers, and supervisors. Characteristics of interest would include the following: resistance to change (Cappelli et al., 2007), maliciousness, egotism, sadism, dishonesty, risk-taking, instability, and lack of strength of character, self-control, or social skills (Tuglular, 2000). The investigators should also look into past instances where the individuals exhibited a strong and unhealthy need for revenge, for recognition, to prove their talents, or to boost their self-confidence (Casey, 2004). Supervisor and co-workers can also help to gaining this insight as they work most closely with the individual.

4.4.8 Role of the Supervisor

A mitigation strategy that the USAF should emphasize and state in policy is the development of a strong working relationship between supervisors and their supervisees. Professionally, supervisors should understand what goals and expectations their supervisees have; as mentioned earlier unmet expectations can lead to disgruntlement (Cappelli et al., 2007). This could be accomplished during the routine evaluations that the USAF currently requires. Ideally, supervisees would feel comfortable expressing concerns with their supervisors instead of planning sabotage. On the personal side, supervisors should check in with their supervisees to see if there are any stressful events going on in their lives. Often stress from outside the workplace filters in and affect one's job performance. It is especially important for supervisors to talk with supervisees if they are acting out of character or if the supervisors have learned about the occurrence of stressful events. Supervisors should also be on the lookout for any relationships their supervisees have with co-workers who could have a negative influence on them. While intervention can be challenging, it is best to act early and hopefully prevent the problem from escalating. If employees are not comfortable talking with supervisors, the supervisors can recommend other resources, such as mental health professionals or the chaplains.

As stated earlier, one-time incidents related to alcohol or poor judgment are not included in SIFs. This is concerning due to how frequently USAF personnel change jobs and supervisors. An employee could habitually be involved in this type of behavior, but if each occurrence is detected by a new supervisor, then it is never recorded. Information regarding poor duty performance is also not kept in SIFs. Though this can be due to lack of ability or training, it can also be due to employees no longer caring about their jobs. It can be the first sign that they are disgruntled and planning to harm the organization (Puleo, 2006). These behaviors are important for supervisors to take notice of and monitor.

Supervisors, security clearance investigators, and network professionals all play a role in collecting information related to the insider threat problem, but the information is not always shared or fused. In the absence of such a system or process, the supervisor can be an important integrator of detectable behaviors. The supervisor can also assist in gaining insight into the insider's personality as the supervisor interacts with the individual more than most others in the organization. The supervisor is essentially the first line of defense in mitigating this problem.

4.4.9 Documenting Insider Threat Controls

While the DoD and USAF policies discuss many controls which are in place to help mitigate the insider threat problem, there are very few explicit references to "insider threat," "espionage," or "sabotage." To show its efforts in protecting against such attacks, the USAF may want to indicate these clearly in more of its policies. The USAF could also publish a separate policy or publication centered on insider threat as it does for counterintelligence (Department of the Air Force , 2000).

4.5 Additional Best Practices for All Organizations

In addition to the recommendations specifically for the USAF, this research purposes three new best practices that supplement those published by the CMU CERT technical staff and similarly can be adopted by any organization. These were developed after comparing the current best practices to published variables and models, historical case studies, the DoD and AF policies that were reviewed, and the models developed for this research, especially the Insider Threat Model for Sabotage and Espionage.

4.5.1 Screen for prior concerning behavior and technical actions, as well as personal dispositions

The best practices published by the CMU CERT technical staff address monitoring for both concerning behavior and technical actions, but only once the insider is a part of the organization. There is no discussion about trying to identify prior inappropriate behaviors or incidents. There is also no recommendation for gaining insight into the insider's personality (such as maliciousness, egotism, and resistance to change) and needs (e.g., for revenge, for recognition, to prove their talents, or to boost their self-confidence) (Tuglular, 2000; Casey, 2004). While this may be difficult to accomplish, it is advisable to attempt to do so during the interview or background investigation process.

United States government agencies, to include the military, use the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" during their background investigations. These guidelines require the investigation to cover such areas as past criminal activity, allegiance to the United States, addictions, sexual behavior, financial responsibility, and inappropriate handling of information and information systems. The investigator also acquires a picture of the individual's past personal conduct, to include incidents related to disloyalty, dishonesty, unreliability, untrustworthiness, lack of sound judgment, irresponsibility, lack of candor, disruptive or violent behavior, and unwillingness to comply with rules and regulations.

This best practice relates to the following variables in the Insider Threat Model for Sabotage and Espionage: *Personal Dispositions, Personal Needs,* and *Detecting Concerning Behavior and Technical Actions*. These are highlights in green in the Insider Threat Model for Sabotage and Espionage, repeated in Figure 24 for convenience.

4.5.2 Issue sanctions to employees for inappropriate technical acts

The best practices published by the CMU CERT technical staff recommend issuing sanctions for inappropriate employee behavior. While the best practices discuss informing employees of the repercussions of violating security measures, they do not address the issuing of sanctions for such violations. Responding to inappropriate or unauthorized technical acts is an important measure in preventing additional and possibly worse incidents from occurring. If malicious insiders are detected and disciplined, they may become less motivated to attack a second time as their risk adversity is increased (Band et al., 2006). Even if the act is fairly innocuous or appears accidental, employee intervention should occur. The seemingly benign incident could be caused by a malicious insider who is testing the strength of the security controls (Stanton et al., 2005). Additionally, even an accidental incident can cause damage. Documentation should supplement the sanctions to aid the detection of a pattern, should it develop. Users of an organization's network should be held accountable for acts they commit that degrade its

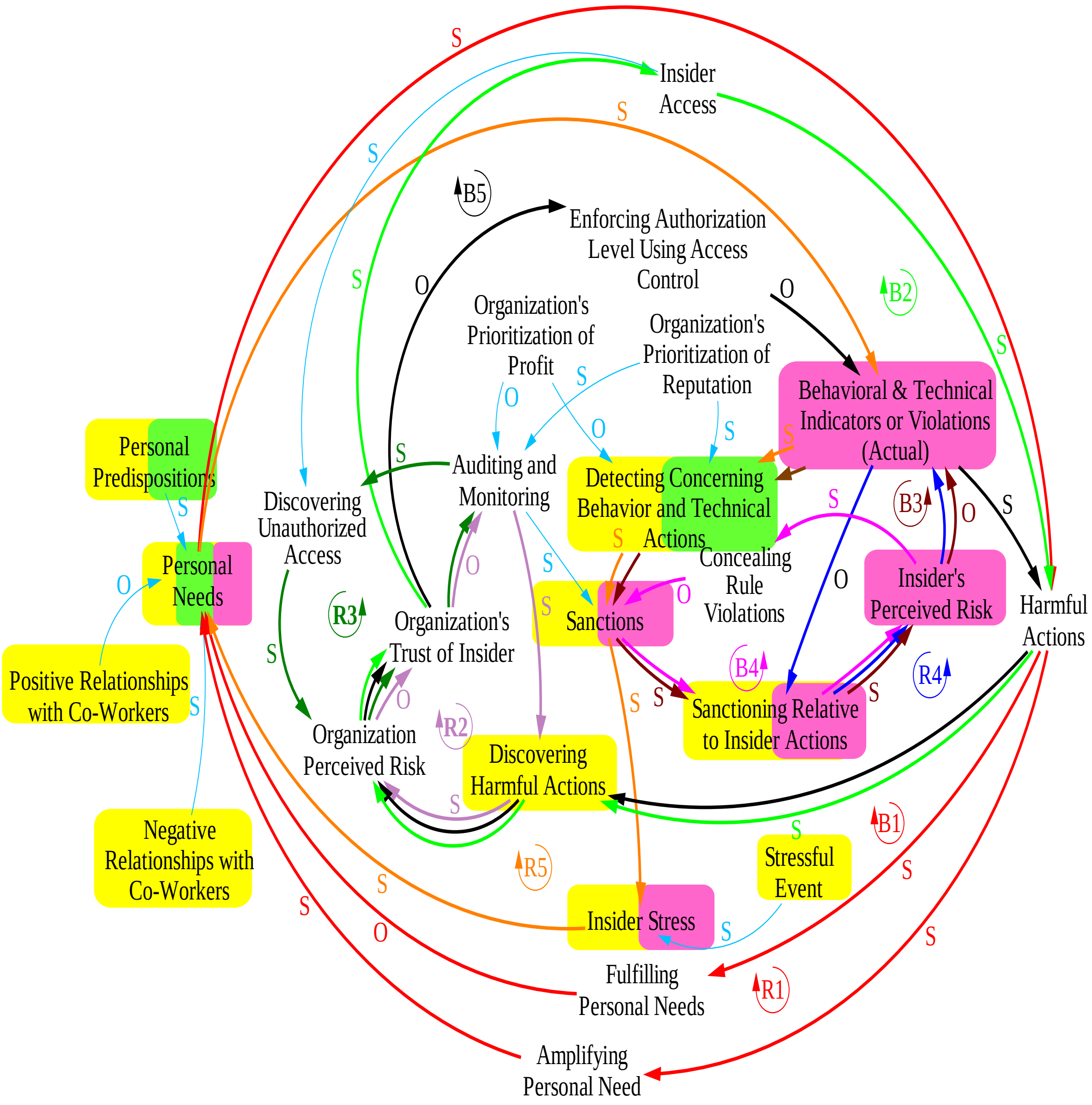

Insider Access
B5
Enforcing Authorization Level Using Access Control
B2
Organization's Prioritization of Profit
Organization's Prioritization of Reputation
Behavioral & Technical Indicators or Violations (Actual)
Personal Predispositions
Auditing and Monitoring
Discovering Unauthorized Access
Detecting Concerning Behavior and Technical Actions
Personal Needs
B3
Insider's Perceived Risk
Harmful Actions
Concealing Rule Violations
Sanctions
R3
Organization's Trust of Insider
Positive Relationships with Co-Workers
B4
R4
Sanctioning Relative to Insider Actions
Organization Perceived Risk
R2
Discovering Harmful Actions
Negative Relationships with Co-Workers
B1
Stressful Event
R5
Insider Stress
Fulfilling Personal Needs
R1
Amplifying Personal Need

Figure 24. Insider Threat Model for Sabotage and Espionage

security and safety. It is important to note that disgruntled insiders may become even more upset if issued sanctions. Intervention, perhaps by the supervisor, may be beneficial to supplement the discipline.

The USAF does discipline its employees for acts that harm or risk the security of the network and information systems. Sanctions include restricted access to controlled areas and information and suspension or loss of a security clearance.

This best practice relates to several of the variables in the Insider Threat Model for Sabotage and Espionage, to include *Sanctions*, *Sanctioning Relative to Insider Actions*, *Insider's Perceived Risk*, *Behavioral & Technical Indicators or Violations (Actual)*, *Insider Stress* (in terms of disgruntlement), and *Personal Needs* (in terms of motivation). These are highlights in magenta in the Insider Threat Model for Sabotage and Espionage (Figure 24).

4.5.3 Require supervisors to take a proactive role

Though the CMU CERT technical staff's best practices addresses training supervisors to detect and respond to concerning behavior, the vital role of the supervisor as an integrator is not captured. In addition to monitoring for suspicious behavior, the supervisor should look for signs of stress, especially if the supervisor is aware of the occurrence of stressful events. Supervisors work closely with their supervisees and may be able to gain insight into their personalities, predispositions, needs, and relationships within the organization. The supervisor can also work to keep the insider's expectations at a realistic level and hopefully alleviate disgruntlement (Cappelli et al., 2007). The supervisor should have access to personnel records; of particular interest is any pattern of concerning behavior. Additionally, the supervisor needs to properly issue sanctions for inappropriate or unauthorized behavior and document these in the insider's records. The supervisor is the first line of defense and plays a significant role in mitigating insider threat.

The USAF policies discuss the storing of unfavorable information in an employee's SIF. Incidents related to theft, family abuse, unauthorized use of weapons, and embezzlement are examples of what can be included in this repository. The SIF is a tool used to determine an employee's eligibility for access to classified information.

This best practice relates to several of the variables in the Insider Threat Model for Sabotage and Espionage, to include *Personal Dispositions*, *Positive Relationships with Co-Workers*, *Negative Relationships with Co-Workers*, *Personal Needs*, *Discovering Harmful Actions*, *Detecting Concerning Behavior and Technical Actions*, *Sanctions*, *Sanctioning Relative to Insider Actions*, *Stressful Events*, and *Insider Stress*. These are highlights in yellow in the Insider Threat Model for Sabotage and Espionage (Figure 24).

4.6 Summary

This chapter explained the methodology of the content analysis conducted on the DoD and USAF policies, to include a description of the CMU CERT's best practices. This chapter also discussed the results of the review; key actors, tools, and areas of focus were identified in addition to shortfalls and conflicts. Recommendations were presented that the USAF could implement in order to better prevent, detect, and respond to malicious insider attacks. Lastly, the chapter discussed three new best practices aimed at helping all organizations with this complex problem.

V. Conclusions

5.1 Summary of the Problem

This research showed how significant the insider threat problem currently is for all organizations. In addition, the difficulty of the problem was explained, to include a discussion of the fact that there is no definitive profile for malicious insiders, organizations have placed trust in these individuals, and insiders have a vast advantage of knowing their organization's personnel, security policies, and information systems.

This research covered many aspects of the insider threat problem, to include common psychological, professional, legal, and economic characteristics and behaviors of malicious insiders, as well as technical precursors which have been documented in historic attacks. The roles played by an insider's expectations, insider's motivations, event triggers, and social networks were analyzed as well. In addition, factors attributed to the organization, such as controls, priorities, and trust, were discussed.

In order to review the USAF policies against the most appropriate model, this research conducted insider threat modeling. Initially a logical data model and a system dynamics model were developed based on previous models from Tuglular (2000) and the CMU CERT technical staff. Once that was accomplished, the Abstracted Common Model was chosen as the basis of this research's Insider Threat Model for Sabotage and Espionage, due largely to its abstractness and inclusion of both espionage and sabotage. There was also an explanation of the incorporation of motivations, organizational priorities, and social networks into this research's final model. These three variables all play significant roles in the insider threat problem and were shown to be relevant to the USAF.

The DoD and USAF polices were reviewed in terms of how well they addresses both the variables of the Insider Threat Model for Sabotage and Espionage and the best practices published by the CMU CERT technical staff. The results of the policy review were presented, focusing on shortfalls and conflicts. This research offered actionable recommendations that the USAF can implement in order to better prevent, detect, and respond to malicious insider attacks. The most significant area for improvement is the utilization of its workforce. All personnel should be trained on observable behaviors that can be precursors to malicious activity. Additionally, supervisors need to be empowered as the first line of defense, monitoring for stress, unmet expectations, and disgruntlement. In addition, this research proposed the following best practices that can be used by any organization to mitigate this threat to security: screening for prior concerning behaviors, predispositions, and technical incidents, issuing sanctions for inappropriate technical acts, and requiring supervisors to take a proactive role.

5.2 Thesis Conclusions

Mitigating the threat from malicious insiders necessitates a solution that involves people, processes, and technology. The USAF is indeed utilizing technology to protect itself against insider attacks. The policies outline the use of such tools as intrusion detection systems, network activity monitoring devices, virus signatures, and strong encryption. One recommendation in this area is to utilize hash functions to compare the baseline and current state of files to detect alterations.

The USAF also has many strict policies in place to mitigate this problem, covering such as topics as strong passwords, least privilege, extra caution with privileged users, backup plans, and access control. The USAF also conducts extensive background checks on its employees, following the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information." This research did have several recommendations in this area, to include more detailed procedures regarding account deactivation, remote access, and privileged users and actions. Additionally, the USAF needs to limit the power of a single individual; this can be done by increasing the separation of duties and not just for technical procedures. Frequent and random checks for bogus accounts ("back doors") should be conducted as well. Additional guidance for auditing could help to improve this area of weakness, to include for which activities to look, how often logs are reviewed, and how long logs should be maintained. Lastly the steps of evaluating controls and determining likelihood and impact need to be included in the risk management process. It is also important that leadership is involve in this assessment as the leaders have greater insight into mission impact than those working solely on network operations.

The USAF's largest area in which it could improve is in utilizing its workforce to help fight against this problem. First of all, all employees should receive training and awareness regarding insider threat. Areas of focus should include tactics that may be directed at them, such as social engineering, and suspicious behavior which they can help detect and report. It is also important that all employees are aware of their organization's security policies. This understanding enhances the likelihood of the policies being followed and therefore improves their effectiveness. The knowledge may also deter potential malicious insiders if they understand all the controls in place, such as monitoring and sanctions. Training could include discussion-based workshops during which co-workers run through scenarios to practice identifying the observable behaviors and actions. Supervisors additionally need to develop relationships with their supervisees in order to help reduce unmet expectations, disgruntlement, and stress. It is also important for supervisors to document concerning behaviors and events, as well as ensure sanctions are issued (e.g., employee intervention or restriction of access). Lastly, supervisors and co-workers can both help the organizations in gaining insight into the other insiders' personalities and needs as they work most closely with them.

5.3 Impact of this Research

Given how significant the insider problem is and how damaging a successful attack could be, the shortfalls identified in this research should be of concern to the USAF. By suggesting solutions, this research hopes to assist the USAF in improving its stance against malicious insiders. The new recommended best practices can aid all organizations in mitigating this threat.

5.4 Possibilities for Future Research

While this research examined 19 DoD and USAF documents from the communications, IA, personnel security, and special investigations arenas, this review was certainly not exhaustive. Additionally, there will certainly be new policies and directives that will be published in the future that could be examined in terms of how they help to mitigate this problem. Additionally, during the September 2008 interview

(Cappelli and Moore, 2008), the CMU CERT technical staff members said they were working on an updated version of the "Common Sense Guide to Prevention and Detection of Insider Threats" (Cappelli et al., 2006). Once this is released, there will mostly likely be new best practices that could be compared to the DoD and USAF policies.

While this research chose to use the Insider Threat Model for Sabotage and Espionage for a content analysis, other tests or analyses could have been run. For example, the model could be compared to a single case study, such as the Hanssen or Lloyd case, or a multitude of cases to see how well it captures the variables in real insider attacks.

Since there is no definitive profile and many of the warning signs are in the form of humanly observable behaviors, organizations are still dependent on humans to prevent attacks. As discussed in the conclusions, the most important mitigating factors are human beings. As mentioned in Chapter IV, supervisors are vital players in detecting these behaviors. An area for further examination is the integration of insider threat mitigation strategies into the training given to new supervisors. Currently, the training includes subject areas such as conduct, discipline, and performance management for which insider threat information could possibly be incorporated (Drake, 2009).

Future research could also work to make progress in information systems having the ability to sense and analyze activities and behaviors, with the goal being to attempt to automate human reasoning. Ideally, if these systems felt that a particular user was a threat, they could alert leadership within the organization and possibly execute an automated response, such as denying the user further access to information systems.

The six different motives (Casey, 2004) examined in this research are not exclusively related to the insider threat problem, or even solely to information security. These motives have been used to gain insight into criminal behavior in general. Similarly, there may be other criminology research and models which could shed light onto the insider threat problem.

Lastly, the insider threat problem could be examined in terms of force protection concepts since it is inherently a security issue. There could be fundamental security concepts that have not yet been applied to its mitigation.

Appendix A: Detailed Policy Review

1. Institute periodic enterprise-wide risk assessments.
    - Actors- DoD CIO, DISN DAA, Heads of DoD components, AFCA, AFIWC, 92 IWAS, AFOSI, AFNOSC, NCC, wing and base host units, MAJCOM, NAF, and wing IA offices/programs/personnel, program/project managers, CND personnel, ISSO
    - Areas of Focus- DoD enterprise-wide, DoD component-level systems, base-level, ports/protocol management, interconnected systems, enclaves, individual IS, software (including patches), hardware, directives/technical orders/specifications, configuration settings, architecture, system life-cycle documents, wireless, biometrics, CONOPS, training and awareness programs
    - Tools- DoD CIO Annual IA Report, DoD uniform risk criteria, adjudicative process, IAVAs/IAVBs, C&A process, AFOSI-provided information, AFCA and other independent audits/assessments (to include Scope EDGE and 92 IWAS red teams), self-assessments, documented threats/vulnerabilities, trend analysis, software tools, Vulnerability Assessment Tool, network vulnerability or penetration testing, scans, logs, IA security incidents and patterns
    - What is covered?
        - Aspects of risk assessment from DoD CIO to NCC to individual systems
        - Analysis of threats, vulnerabilities, controls, risk
        - Feedback/communication between levels
        - Hierarchical structure
    - What are the shortfalls?
        - Likelihood determination
        - Impact determination
    - What are the conflicts? None
    - What are recommendations?
        - Determine likelihood and impact
        - Prioritize critical assets

2. Institute periodic security awareness training for all employees.
    - Actors- DoD CIO, SAF/XCI, Director of NSA, Heads of DoD components, HQ USAF/IL, HQ USAF/ILCO, HQ USAF/ILCX, AETC, United States Air Force Academy, AFPC, AFOSI, AFCA (AFCA/WFP), MAJCOM functional manager, MAJCOM & wing IA offices/programs, wing/base host commanders/SC/units, Air Force Field Operating Agencies and Direct Reporting Units, unit commanders, unit IA awareness managers, Functional Systems Administrator, workgroup managers, DAA, ISSM/O, certifier (in C&A process), users/network professionals (to include military, civilian, guard, reserve, government contractors, foreign national employees)

- Areas of Focus
  - Current, engaging, and relevant to the target audience to enhance effectiveness; influence behavior; focus must be on actions that empower the user; must understand critical reliance on IS & that they are a critical link in IA posture
  - Unauthorized or illegal use of computer hardware and software
  - Potential harm to national security due to the improper use of information systems
  - Consequences if policies and procedures are not followed
  - Communications, network, emission, computer security
  - Identification and authentication; password construction
  - Internet "do's and don'ts"
  - Threats, vulnerabilities & countermeasures concerning tampering, disclosures, modification, destruction, denial of service, fraud, misappropriation, misuse, access by unauthorized persons, social engineering, malicious code
  - Safeguarding information processed, stored, or transmitted on all these systems
  - Availability, integrity, authentication, confidentiality, and non-repudiation
  - Privacy rights & consent to monitoring
  - Security responsibilities
    - Responding to and reporting suspicious activities and conditions; h
    - Protecting information and IT they access;; copyright, ethics, and standards of conduct; malicious code; prevent self-inflicted damage
  - Insider threat specific
    - 'Insider threats'
    - Social engineering
    - Countermeasures to protect systems and information from sabotage & espionage
    - Examples of internal threats such as malicious or incompetent authorized users, users in the employ of terrorist groups or foreign countries, disgruntled employees or Service members, hackers, crackers, and self-inflicted intentional or unintentional damage
    - Threat posed by foreign intelligence, foreign government-sponsored commercial enterprises, all pertinent terrorist threats, and international narcotics trafficking organizations
- Tools
  - Air Force IA Home Page (https://private.afca.af.mil/ip)
  - DoD CIO Annual IA Report
  - Training/Courses- Air Force Information Assurance Awareness Training" Computer-Based Training (CBT), resident courses,

distributive or blended training, SOJT, exercises, certification/recertification

      - Initial military training- basic military training, Officer Training School, Air Force Reserve Officer Training Corps, and specialized training in Air Force Specialty Code (AFSC)-awarding courses
      - Air University courses- formal schools and professional military education courses
      - Civilian career programs
    - Counterintelligence Awareness Briefings
    - Awareness materials- briefings, pamphlets, flyers, posters, base bulletins, trifolds, screen savers, and videotapes
    - Increased depth for students' who may become involved in planning, programming, managing, operating, or maintaining information systems
    - Assessments of training
- What is covered?
    - Try to grab everyone when I first begin working with military
    - Annual refresher
- What are the shortfalls?
    - Unaware of website & AFOSI briefs
    - Quality of training/method used- effectiveness of CBT
    - Often refer to "IA training"- few specific references to "insider threat"
    - Need to discuss behaviors so employee know what to look for and they can report
    - Tie between SE and IT
- What are the conflicts?
    - We say users are "critical link" but the importance of this issue is not stressed
- What are recommendations?
    - Enhanced training- discussion-based, video game, red team outbriefs shared with more people
    - IT material stressed and importance of every user- reportable behaviors
    - Tie between SE and IT

3. Enforce separation of duties and least privilege.
    - Actors- Heads of DoD components, AFNOSC, NOSC, wing IA offices, Top Secret Control Office, IAM, IAO, ISSM, ISSO, SA, authorized users,
    - Areas of Focus- DoD enclaves; Top Secret material; Top Secret Control Account; TCNOs; privileged users and access, privileged programs (OS, system parameter and configuration files, and databases); privileged utilities (assemblers, debuggers, and maintenance utilities); security-relevant programs/data files (security monitor, password files, and audit

files); web sites containing official information; intelligence, proprietary, and control information; software/hardware/firmware; joint and coalition partners, Voluntary Emeritus Corps

- Tools- None
- What is covered?
  - Obvious focus on TS, classified, privileged access
  - Does cover broad issues of need-to-know
- What are the shortfalls?
  - IA functions, TCNOs & Top Secret Control Account inventory were only specific activities with two-person compliance
  - Only information system activities covered
- What are the conflicts? None
- What are recommendations?
  - Would think more NOSC/NCC functions would be prime to implement two-person compliance
  - Need to make sure one person cannot be secretly doing things on the network
  - Applied to functions other than info systems

4. Implement strict password and account management policies and practices.
   - Actors- NOSC, Red and Blue Team personnel, NCC, SA, FSA, unit security manager, CSA,WGM, ISSO,
   - Areas of Focus-
     - Assign/maintain/delete user IDs/passwords/privileges, suspended/transferred/terminated personnel, locking/unlocking accounts, resetting passwords, updating e-mail addresses, one-time password, password composition, dormant accounts, rapid retries
     - Individual accountability, reusable generic/group usernames, non-repudiation, shared use of data
     - Limit elevated privileges (service accounts, , loading new users, password management, modifying and patching system routines or files, examining memory locations, real-time monitoring of user activities, trusted profile (e.g., system administrator, security officer, root user, super user, backup operators)
     - Remote session, password cracking, compromised passwords, enclave, encryption, wireless, SNMP management
   - Tools- favorable background investigation, Personnel Security Management Program, proper security clearance, two-factor authentication, hardware tokens, PKI, policies, automated procedures (i.e. via OS), password enforcement software, i-TRM password cracking tools, IA program/annual training, assessments
   - What is covered?
     - Two of the most important issues
       - individual accountability
       - non-repudiation

        - Strong identification/authentication
        - Monitoring accounts
        - Actively searching for weaknesses
        - Good they focus on privileged acct
    - What are the shortfalls?
        - Humans- SE, laziness, writing down passwords, sharing passwords
        - No explicit check for creation of bogus accounts
            - Yes, solid policies for granting an account (clearance, background check, training), checking for dormant, and terminating personnel who are leaving but what about checks on the people doing this (CSA, SA)—should be another person comparing accounts with valid users
            - CMU- need to prevent backdoors
    - What are the conflicts? None
    - What are recommendations?
        - Push for biometrics & increased use of PKI
        - Training
            - current- composition, identification/authentication
            - need SE, diligence, not sharing
        - Account checks- should be done frequently but randomly (CMU quote)

5. Log, monitor, and audit employee online actions. Collect and save data for use in investigations.
    - Actors- ISSM, ISSO, SA, Heads of DoD components, DoD Component IA program, IAT Level II Personnel, CND-A, CND-AU, AFOSI
    - Areas of Focus-
        - Weak configurations, security holes/deficiencies,
        - Core network services and infrastructure devices, VPN tunnel, system services for authentication
        - Incidents, unusual/inappropriate activity
            - Changing the security profile (e.g., access controls, security level of the subject, user password)
            - Successful/unsuccessful log-in attempts, file system modifications, change in privileges
            - Attempted/realized penetrations/intrusions, unauthorized transmissions, unauthorized attempts to bypass automated information systems security devices or functions, unauthorized requests for passwords, or unauthorized installation of modems or other devices into automated information systems (including telephone systems) whether classified or unclassified
        - Inform users via consent to monitoring, associating the user's identity with all auditable actions

  - Unencrypted (clear text) passwords, incorrectly entered passwords, or character strings; access to the audit trail file; info directly to the user
- Tools- audit/monitoring/error/host/network traffic/firewall/intrusion detection logs/files, intrusion detection tools, deployable CND audit toolkit, IS aborts/suspends unauthorized user activity
- What is covered?
  - Checking individual system, network activity (log-in, modifications), firewall
  - Includes special mention of VPN—good since insiders often use
  - Attributing each action to a individual
  - Suspicious activities- file modifications, privilege/security changes, unauthorized transmissions, bypasses
- What are the shortfalls?
  - Training/awareness- consent to monitoring
  - Additional suspicious activity to look at
    - sudden change in activity (working earlier/later, printing/transmitting more files, accessing files they don't need for work)
    - would require creating baselines
  - Lots of discussion of collect but nothing that I saw about saving (how long, format, etc)
- What are the conflicts?
  - Do we have the time and manpower to do all this and even more with personnel and budget cuts?
- What are recommendations?
  - Training/awareness- want to tell them what is being looked at specifically
  - Guidance on cataloging/storing logs and reports
  - Create baselines if monitoring more activities

6. Use extra caution with system administrators and privileged users.
   - Actors- Heads of the DoD Components, Wing IA Office, IAM, commanders and or supervisors
   - Areas of Focus- contractors, Automated Information Systems (increased monitoring), separation of functions, personal accounts with domain administrative privileges, passwords, i-TRM password cracking tools
   - Tools- favorable National Agency Check, local agency check, and credit check, written inquiries, investigations, DOD issued PKI certificates/ hardware tokens, preparatory & sustaining DoD IA training and certification requirements, Privileged Access Agreement,"
   - What is covered?
     - Background checks
     - Separating personal and privileged accounts
     - Separation of functions

- What are the shortfalls?
    - o “Maintain visibility” is very passive
    - o “Extra monitoring” for AIS- vague
- What are the conflicts? None
- What are recommendations?
    - o Explicit policies for monitoring sys admin (checks and balances)
        - ▪ User account creation, modifications, running scripts, recommended policy changes, modifying logs

7. Actively defend against malicious code.
    - Actors- HQ AFCA/EVP, AFIWC, AFNOSC, NOSC, NCC, Information Protection Operations personnel, CND- IS, CND-A, program manager, DAA, ISSO, CSA, authorized users
    - Areas of Focus- wireless, web sites, E-mail, rules/signatures, freeware/firmware/shareware/public domain software, timeliness of changes, removable and fixed media
    - Tools- AFCERT/DoD CERT sites, CSAP Database System, antivirus tools/signature files/software, software patches and security fixes, user awareness training, local policies, configuration management, virus scan, malicious logic reports
    - What is covered?
        - o Strength- signature-based
        - o Big focus on viruses
        - o Help from above
        - o Looking at array of mediums (software, e-mail, websites)
        - o Taking a lot of control out of the hands of normal user
    - What are the shortfalls?
        - o Weakness- statistical-based
        - o No baselines of configurations
    - What are the conflicts?
        - o Baselines can be expensive to create and update
        - o May need various types depending on user role
    - What are recommendations?
        - o Create hashes of baselines of both software and hardware configurations so you can detect a change (such as hash functions of key files- windows explorer and task manager)

8. Use layered defense against remote attacks.
    - Actors- NOSC, NCC, ANG NCC, IAM, IAO
    - Areas of Focus- back-door access, additional network interface (modem, wireless, etc.), privileged access, High Impact PII electronic records, disconnecting dormant session, encryption
    - Tools- VPN client software, access tables, audit logs, NIST-certified cryptography, proxy services, screened subnets, DMZ

- What is covered?
    - Restrictions on privileged actions and sensitive info
    - Maintaining logs (increased attention to privileged actions)
    - Call-forwarding
- What are the shortfalls?
    - Does not spell out who validates need for remote access
    - Does not discuss termination of accts- hopefully the same as other accounts
- What are the conflicts? None
- What are recommendations?
    - Explicitly spell out who grants permission to remote access
    - Explicitly spell out policy on disabling with termination of role "discouraged"

9. Monitor and respond to suspicious or disruptive behavior.
    - Actors- AFOSI, Central Adjudication Facility, commanders, security officials, NCC OIC, IAO, AF Government Charge Card program coordinators, authorized users,
    - Areas of Focus-
        - Theft, embezzlement, bankruptcy petitions, indebtedness
        - Unauthorized sale or use of firearms, explosives/dangerous weapons, alleged criminal activity
        - Child or spouse abuse, child advocacy reports
        - Misuse or improper disposition of government property or other unlawful activities, Government Charge Card abuses and misuses,
        - AFOSI reports of investigation; civil/police/security forces incident/complaint reports; administrative/disciplinary actions to include records of counseling, letters of reprimand, Article 15, Uniform Code of Military Justice (UCMJ), or courts-martial orders
        - Medical or mental health evaluations
        - Action that threatens the security of, or damages/harms network or government communications systems, IA-related events and potential threats and vulnerabilities involving a DoD information system
        - Foreign intelligence or any terrorist organization may have targeted for possible intelligence exploitation, request for illegal or unauthorized access to classified or unclassified controlled information, contact with a known or suspected intelligence officer, contact with foreign diplomatic establishment, suspected espionage, terrorism, spying, treason, unlawful intelligence activities, sedition, subversion
        - Sabotage, unauthorized technology transfer, contemplated/ attempted/effected the deliberate compromise or unauthorized release of classified or unclassified controlled information

- Tools- security information file, information assurance policies, special investigation policies
- What is covered? criminal activity, technical precursors, financial, problems in family,
- What are the shortfalls?
    - Acting out of character, alarming statements
    - Foreign travel- does discuss relationships with foreign people, especially intelligence personnel or terrorists
- What are the conflicts?
    - Poor duty performance- sign that they no longer care, will harm organization
    - Following could be early signs or mean more when pieced together- disciplinary issues, one-time alcohol related incident, single isolated incident of poor judgment based on immaturity or extenuating circumstances
- What are recommendations?
    - Should definitely include poor job performance, especially if it was good and has worsened (to include tardiness, absences, not meeting deadlines, quality of work)
    - Need to look at alcohol incidents and any other addictions (gambling)
    - Also include unusual behavior, signs of stress

10. Deactivate computer access following termination.

- Actors- NCC, NOSC, SA, WGM, CSA, FSA
- Areas of Focus- E-mail account, SNMP management, user accounts
- Tools- procedures
- What is covered? E-mail, SNMP, user accounts
- What are the shortfalls?
        - "Ensure procedures are in place" is quite weak
        - E-mail still available for 60 days—could send a virus—would most likely be trusted
- What are the conflicts? None
- What are recommendations?
    - Standard, strict procedures to ensure deletion or all accounts and privileges
        - Spell out checking SA, database, remote access, and other privileged accounts
    - Shorter (or no grace period) with e-mail

11. Implement secure backup and recovery processes.

- Actors- AFNOSC, NOSC, NCC, IA Officer, IAT Level III Personnel, IA Manager (IAM) Level I Personnel

- Areas of Focus- IA requirements/features/procedures, NCC managed servers, NOSC managed core services, enclaves
- Tools- Continuity of Operations Plan, quarterly tests, monitoring by IA officers, assistance from AFNOSC
- What is covered?
  - Good that there is help from above
  - Daily backups for their systems
  - Procedures/plans/COOP
  - Quarterly tests
- What are the shortfalls?
  - Vague
    - Redundancy?
    - Ghost images?
- What are the conflicts? None
- What are recommendations? More concrete plans—perhaps do not have those in public domain

12. Analyze current access control policies and practices and identify and evaluate options to mitigate insider threat risk.
    - Actors- USAF/CVA, AFIWC/IO, AFNOSC, MAJCOM/CC or MAJCOM NOSCs, FSA, DAA, ISSO, unit commanders, IAO, Foreign Disclosure Office, authorized users
    - Areas of Focus-
      - Individual Ready Reserve, vendor maintenance personnel, contractors, foreign nationals, volunteers, summer-hire employee, privileged user with IA responsibilities
      - Classified/controlled unclassified information/media/products, SIPRNET, remote access, shared files, stand-alone system, enclaves, AIS applications, outsourced IT-based processes, platform IT interconnections, specialized CND systems (e.g., firewalls and intrusion prevention systems)
      - Backdoors and unauthorized connections, building and area entry controls, interim access, deleting access
    - Tools- level of the position, identification/authentication/authorization, mission needs, clearances, favorable trustworthiness investigation, supervision, user licensing, IT position category requirements and qualifications, IA awareness and training, need to know, sanitization, network components using MAC, Access Control Lists, classification level of the information, mission assurance category, security domain, releasability/sensitivity of information, SSAA
    - What is covered?
      - Special users- foreign nationals, privileged users, volunteers, etc
      - High-risk items- SIPRNET, classified, controlled, special systems
      - Policies- Identification/authentication, clearances, need-to-know, mission

  - What are the shortfalls? Only mention of checking ACLs is to “manage” or “update” for CND & SDP routers
  - What are the conflicts? None
  - What are recommendations?
    - ACLs- should be reviewed randomly and often, looking for oversights and phony/backdoor accounts

13. Clearly Document Insider Threat Controls
  - Actors- No explicit but incorporated into the above controls
  - Areas of Focus- No explicit but incorporated into the above controls
  - Tools- No explicit but incorporated into the above controls
  - What is covered?
    - Limited training/awareness
    - Limited reportable behavior
  - What are the shortfalls?
    - Many listed above
  - What are the conflicts? See above
  - What are recommendations?
    - Above recommendations
    - Perhaps its own section within instructions
  - Sanctions (for inappropriate technical acts)
    - Actors- CAF, commander, DAA, CSA
    - Areas of Focus- access to classified information, SCI and SAP access, unescorted entry to restricted areas, security clearance, license suspension
    - Tools- SIF, determination if individual is threat to network, licensing principles (failure to maintain an acceptable level of proficiency on a critical program; actions that threaten the security of a network or a governmental communications system; actions that may result in damage or harm to a network or governmental communications system; or actions that constitute unauthorized use under the provisions of AFI 33-119, Air Force Messaging, or AFI 33-129, Web Management and Internet Use)
    - What is covered?
      - Suspension, loss of clearance, access to information/resources
      - Looks at SIF, licensing principles
    - What are the shortfalls?
      - Employee intervention
    - What are the conflicts?
    - What are recommendations?
      - Intervention to limit disgruntlement—need to get at root of problem

- Organization's Prioritization of Profit
  - Actors- None
  - Areas of Focus- None
  - Tools- None
  - What is covered? Not covered
  - What are the shortfalls? None
  - What are the conflicts?
    - AF is not profit-oriented so should be willing to spend more on controls but we are restricted by federal budget
  - What are recommendations? None

- Organization's Prioritization of Reputation
  - Actors- None
  - Areas of Focus- None
  - Tools- None
  - What is covered? Not covered
  - What are the shortfalls? None
  - What are the conflicts?
    - We should be highly concerned with reputation, again making us want to invest in controls (but have budget that restrains us)
  - What are recommendations? None

- Organization's Trust of Insider
  - Actors- None
  - Areas of Focus- complete confidence cannot be achieved, access decisions, secure environment, classified information
  - Tools- adjudicative guidelines, risk management
  - What is covered?
    - Risk management approach, critical assets that are of highest importance, background investigations
    - All three categories covered
  - What are the shortfalls? None
  - What are the conflicts? None
  - What are recommendations? None

- Insider Stress
  - Actors- None
  - Areas of Focus- None
  - Tools- None
  - What is covered? Not covered
  - What are the shortfalls?
    - Role of supervisor and co-workers
  - What are the conflicts? None

        - What are recommendations?
            - Supervisor and co-worker responsibility
            - Would not see it in SIF, but intervention is important
            - Co-workers report to supervisor

    - Stressful Event
        - Actors- None
        - Areas of Focus- None
        - Tools- None
        - What is covered? Not covered
        - What are the shortfalls?
            - Role of supervisor and co-workers
        - What are the conflicts? None
        - What are recommendations?
            - If supervisor knows of event should be more on the lookout for changes in behavior
            - Co-workers should report to supervisor

    - Personal Predispositions
        - Actors- Surgeon General, Heads of the DoD Components, Mental Health Clinic
        - Areas of Focus-
            - Sabotage, espionage
            - Criminal conduct- serious offense, several minor, dishonorable discharge, parole/probation,
            - Physical, mental, or emotional conditions
            - Allegiance to the United States- treason, terrorism, sedition, dual citizen and/or possess/use a foreign passport, employment/service to foreign organizations
            - Sexual behavior- criminal, poor judgment
            - Personal conduct- disloyalty, unreliability, untrustworthy, lack of sound judgment, irresponsibility, lack of candor, disruptive, violent, inappropriate behavior in the workplace, dishonesty or rule violations, dishonesty, unwillingness to comply with rules and regulations, breach of client confidentiality
            - Financial considerations- inability to live within one's means, satisfy debts, and meet financial obligations; unexplained affluence
            - Addictions- drug abuse, alcoholism, gambling problems (and related incidents)
        - Tools- SIF, Adjudicative Guidelines
        - What is covered? criminal, mental, US allegiance, addictions, conduct/behavior, financial

  - What are the shortfalls? personality- malicious, egotistical, social skills, resistant to change
  - What are the conflicts? None
  - What are recommendations?
    - Personality profile- from past co-workers, supervisors, friends, family

- Positive Relationships with Co-Workers
  - Actors- None
  - Areas of Focus- None
  - Tools- None
  - What is covered? Not covered
  - What are the shortfalls? supervisors' role
  - What are the conflicts? None
  - What are recommendations?
    - Supervisors especially should be monitoring relationships/influences on their employees

- Negative Relationships with Co-Workers
  - Actors- Background clearance investigators
  - Areas of Focus-
    - Allegiance to the United States- sympathy/association with people committing sabotage, espionage, treason, terrorism, or sedition
    - Association with persons involved in criminal activity
  - Tools- Adjudicative Guidelines
  - What is covered?
    - Allegiance
    - Criminal activity
  - What are the shortfalls?
    - Association with co-workers committing precursory events at work (technical, behavioral)
  - What are the conflicts? None
  - What are recommendations?
    - Supervisors especially should be monitoring relationships/influences on their employees

- Personal Needs
  - Actors- CAF
  - Areas of Focus-
    - Financial considerations- inability to live within one's means, satisfy debts, and meet financial obligations; unexplained affluence, embezzlement, frivolous spending, gambling

    - Foreign influence
      1. Espionage, treason, terrorism, sedition
      2. Substantial business, financial, or property interest in a foreign country
  - Tools- Adjudicative Guidelines
  - What is covered?
    - Foreign & financial influences
  - What are the shortfalls?
    - Need for revenge, recognition, prove themselves, boost one's self-confidence, sadistic, achieve satisfaction
  - What are the conflicts?
  - What are recommendations?
    - Look for these personality characteristics- need for recognition, need to prove themselves, sadistic
    - Look for development of disgruntlement

- Detecting Concerning Behavior and Technical Actions
  - Actors- Background clearance investigators
  - Areas of Focus-
    - Handling protected information- disclosure, copying, storing in unauthorized location, unapproved equipment, outside one's need to know, negligence or lax security habits
    - Use of IT systems- noncompliance with rules, procedures, guidelines or regulations; illegal or unauthorized entry, modification, destruction, manipulation or denial of access; downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system; unauthorized use, introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization; negligence or lax security habits
  - Tools- Adjudicative Guidelines
  - What is covered?
    - This covers initial/historical technical information—rest if covered by monitoring & auditing
  - What are the shortfalls?
    - Behavior- we need to be training our employees on what to look for so they can actually detect it
  - What are the conflicts? None
  - What are recommendations?
    - Training

Bibliography

Band, S. R., Cappelli, D. M., Fisher, L. F., Moore, A. P., Shaw, E. D., and Trzeciak, R. F. (2006). *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis.* Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute.

Blau, G. (1985). Relationship of Extrinsic, Intrinsic, and Demographic Predictors. *Journal of Applied Psychology* , 442-450.

Brackney, R. C., and Anderson, R. H. (2004). Understanding the Insider Threat. *McAfee Security workshop.* Rockville, MD: RAND Corporation.

Butts, J. W. (2006). *Formal Mitigation Strategies for the Insider Threat: A Security Model and Risk Analysis Framework*. MS thesis, AFIT/GIA/ENG/06-02. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson Air Force Base, OH.

Cappelli, D. M., and Moore, A. P. (2008, September 23). Carnegie Mellon University CERT Technical Staff. (E. C. Leach, Interviewer).

Cappelli, D. M., Desai, A. G., Moore, A. M., Shimeall, T. J., Weaver, E. A., and Willke, B. J. (2007). *Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks.* Pittsburgh, PA: CERT Program.

Cappelli, D. M., Moore, A. M., Shimeall, T. J., and Trzeciak, R. F. (2006). *Common Sense Guide to Prevention and Detction of Insider Threats (2nd Edition, Version 2.1).* Pittsburgh, PA: Carnegie Mellon University.

Casey, E. (2004). *Digital Evidence and Computer Crime.* London: Academic Press.

Colombi, J. (Summer Quarter 2008). IMGT 580- Enterprise Information Architecture. Wright-Patterson AFB, OH: Air Force Institute of Technology (AU).

Cooper, R., and Garvey, M. (2001, February 25). Spy suspect: In the end, a soul lost and lonely. *Los Angeles Times* .

CSO. (2007). *2007 E-Crime Watch Survey- Survey Results. CSO Magazine, U.S. Secret Service, CERT Program, Microsoft Corp.* Retrieved April 5, 2008, from http://www.cert.org/archive/pdf/ecrimesummary07.pdf

Department of Defense. (2007). *DoD Architecture Framework Version 1.5, Volume II: Product Descriptions.*

Department of Defense. (2002). *Information Assurance (IA) (DoD 8500.01E).* Washington: GPO.

Department of Defense. (2003). *Information Assurance (IA) Implementation (DoD 8500.02).* Washington: GPO.

Department of Defense. (2005). *Information Assurance Workforce Improvement Program (DoD 8570.01-M)* . Washington: GPO.

Department of Defense Office of Inspector General. (2006a). *Information Technology Management- DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements (D-2006-052).* Washington, DC: Department of Defense.

Department of Defense Office of Inspector General. (2006b). *Information Technology Management- Select Controls for the Information Security of the Ground-Based Midcourse Defense Communications Network (D-2006-053).* Washington, DC: Department of Defense.

Department of the Air Force. (1997). *Computer Security Assistance Program (AFI 33-207).* Washington: HQ USAF.

Department of the Air Force. (2000). *Counterintelligence (AFI 71-101, Volume 4).* Washington : HQ USAF.

Department of the Air Force. (1999). *Special Investigations(AFPD 71-1).* Washington : HQ USAF.

Department of the Air Force. (2004b). *Air Force Network Operations Instructions (AFI 33-115, Volume 3).* Washington: HQ USAF.

Department of the Air Force. (2005c). *Identification and Authentication (AFMAN 33-223).* Washington: HQ USAF.

Department of the Air Force. (2004c). *Information Assurance (IA) Awareness Program (AFI 33-204).* Washington: HQ USAF.

Department of the Air Force. (2007). *Information Assurance (IA) Program (AFPD 33-2).* Washington: HQ USAF.

Department of the Air Force. (2004d). *Information Assurance Assessment and Assistance Program (AFI 33-230).* Washington: HQ USAF.

Department of the Air Force. (2006d). *Information Management (AFPD 33-3).* Washington: HQ USAF.

Department of the Air Force. (2006c). *Information Resource Management (AFPD 33-1).* Washington: HQ USAF.

Department of the Air Force. (2005a). *Information Security Program Management (AFI 31-401).* Washington: HQ USAF.

Department of the Air Force. (2004a). *Licensing Network Users and Certifying Network Professionals (AFI 33-115, Volume 2).* Washington: HQ USAF.

Department of the Air Force. (2006b). *Network and Computer Security (AFI 33-202, Volume 1).* Washington: HQ USAF.

Department of the Air Force. (2006a). *Network Operations (AFI 33-115, Volume 1).* Washington: HQ USAF.

Department of the Air Force. (2005b). *Personnel Security Program Management (AFI 31-501).* Washington: HQ USAF.

Drake, D. (2009). *Supervisory Training Courses.* Retrieved Febrauary 19, 2009, from USAF Portal: https://www.my.af.mil/gcss-af/USAF/ep/contentView.do?contentType=EDITORIAL&contentId=606064&programId=1616747.

Elky, S. (2006, May 31). *Information Security Reading Room*. Retrieved July 16, 2008, from SANS Institute: http://www.sans.org/reading_room/whitepapers/auditing/1204.php

Gladwell, M. (2002). *The Tipping Point- How Little Things Can Make a Big Difference*. New York: Little, Brown and Company.

Grimaila, M. R. (Fall Quarter 2008). IMGT 687- Management Aspects of Information Warfare. Wright-Patterson Air Force Base, OH: Air Force Institute of Technology.

Havill, A. (2001a). *The Last Day In the Sun - Robert Hanssen Story*. Retrieved March 5, 2009, from Tru TV: http://www.trutv.com/library/crime/terrorists_spies/spies/hanssen/1.html.

Havill, A. (2001b). *The Spy Who Stayed Out in the Cold: The Secret Life of FBI Double Agent Robert Hanssen*. New York: St. Martin's Press.

Heinze, A. and Proctor, C. (2004). Reflections on the Use of Blended Learning. *Education in a Changing Environment conference proceedings*. Salford, England.

Herbig, K. L., and Wiskoff, M. F. (2002). *Espionage Against the United States by American Citizens 1947-2001*. Monterey,CA: Defense Personnel Security Research Center (PERSEREC).

Hsieh, H. F., and Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research* , 1277-1288.

Laird, S. K., and Rickard, J. T. (2005, May 3). Retrieved August 2008, from MITRE: https://analysis.mitre.org/proceedings/Final_Papers_Files/99_Camera_Ready_ Paper.pdf

Lee, M. S. (2007). *SIMEN Says: Let's Make Air Force Networks More Secure.* Retrieved February 18, 2009, from *MITRE:* http://www.mitre.org/news/digest/advanced_research/01_07/a_simen.html.

Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., and Stewart, T. R. (2008). A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach. *ACM Transactions on Modeling and Computer Simulation , 18* (2), 7:1-7:27.

Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., Lomgstaff, T., Spitzner, L., Haile, J., Copeland, J., and Lewandowski, S. (2005). Analysis and Detection of Malicious Insiders. *International Conference on Intelligence Analysis.* McLean, VA.

Mayer, R. C., Davis, J. H., and Schooman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review , 20* (3), 709-734.

Mayring, P. (2000, June). *Qualitative Content Analysis.* Retrieved January 26, 2009, from Forum: Qualitative Social Research: http://www.qualitative-research.net/index.php/fqs/article/view/1089/2386

McKnight, D. H., Cummings, L. L., and Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. *Academy of Management Review, 23* (3), 473-490.

McMillan, R. (2009, January 30). *Fired Fannie Mae contractor tried to crash network*. Retrieved February 18, 209, from CSO: http://www.cso.com.au/article/274869/fired_fannie_mae_contractor_tried_crash_network

Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., and Cooke, D. L. (2003). A System Dynamics Model of an Insider Attack on an Information System. In J. J. Gonzalez, *From modeling to managing security: A system dynamics approach* (pp. 9-36). Kristiansand, Norway: Høyskoleforlaget AS - Norwegian Academic Press.

Mills, R. F., Peterson, G. L., and Grimaila, M. R. (2009) Insider Threat Prevention, Detection, and Mitigation. In *Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions*, K. Knapp, editor,. Hershey, PA: IGI Global Publishing.

Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. (2008). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures.* Pittsburgh, PA: CERT Program.

PERSEREC. (2004). *Recent Espionage Cases 1975-2004.* Retrieved September 17, 2008, from Defense Personnal Security Research Center (PERSEREC): http://www.dhra.mil/perserec/EspionageCases1975-2004/2000-04.htm#RobertPhilipHanssen

Phyo, A. H., and Furnell, S. M. (2004). A Detection-Oriented Classification of Insider IT Misuse. *3rd Security Conference.* Las Vegas.

Piccoli, G., Ahmad, R., & Ives, B. (2001). Web-Based Virtual Learning Environments: A Research Framework and a Preliminary Assessment of Effectiveness in Basic IT Skills Training. *MIS Quarterly*, 401-426.

Pipkin, D. L. (2000). *Information Security.* Upper Saddle River, NJ: Prentice Hall PTR.

Puleo, A. J. (2006). *Mitigating Insider Threat Using Human Behavior Influence Models.* MS theis, AFIT/GCE/ENG/06-04. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB, OH.

Rich, E., Martinez-Moyano, I. J., Conrad, S., Cappelli, D. M., Moore, A. P., Shimeall, T. J., et al. (2005). Simulating Insider Cyber-Threat Risks: A Model-Based Case and Case-Based Model. *International Conference of System Dynamics Scoiety*, (pp. 1-28).

Robbins, S. P., and Judge, T. A. (2008). *Essentials of Organizational Behavior.* Upper Saddle River, NJ: Pearson Prentice Hall.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review , 23* (3), 393-404.

Shaw, E., Ruby, K. G., and Post, J. M. (1998, September). *The insider threat to information systems. Security Awareness Bulletin No. 2-98.* Retrieved September 16, 2008, from Department of Defense Security Institute: http://www.pol-psych.com/sab.pdf

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). Analysis of End User Security Behaviors. *Computers & Security , 24*, 124-133.

Sterman, J. D. (2000). *Business Dynamics,* Burr Ridge, IL: Irwin McGraw-Hill.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* Gaithersburg, MD: National Institute of Standards and Technology.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2005). The Insider Threat to Information Systems and the Effectiveness of ISO17799. *Computers and Security , 24*, 472-484.

Trochim, W., and Donnelly, J. P. (2007). *The Research Methods Knowledge Base, 3e.* Mason, OH: Atomic Dog Publishing.

Tuglular, T. (2000). A Preliminary Structural Approach to Insider Computer Misuse Incidents. *EICAR 2000 Best Paper Proceedings* (pp. 105-125). Aalborg, Denmark: EICAR.

Under Secretary for Management. (2006, February 3). *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*. Retrieved Septemeber 15, 2008, from U.S. Department of State: http://www.state.gov/m/ds/clearances/60321.htm.

Ventana Systems, Inc. (2007, July 4). *Vensim User's Guide Version 5.* Retrieved August 21, 2008, from Vensim: http://www.vensim.com/documentation.html.

Vijayan, J. (2008, October 31). *Recession Increases Security Risks, Particularly Insider Threats*. Retrieved February 18, 2009, from CIO: http://www.cio.com/article/458273/Recession_Increases_Security_Risks_Particularly_Insider_Threats.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 26-03-2009	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From – To)* January 2008 – March 2009

4. TITLE AND SUBTITLE

Mitigating Insider Sabotage and Espionage: A Review of the United States Air Force's Current Posture

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Leach, Erika C., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology (AFIT/EN)
Graduate School of Engineering and Management
2950 Hobson Way, WPAFB, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENG/09-05

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Intentionally Left Blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

The security threat from malicious insiders affects all organizations. This problem is difficult due to the fact that there is no definitive profile for malicious insiders, organizations have placed trust in these individuals, and insiders have a vast knowledge of their organization's personnel, policies, and information systems.

The purpose of this research is to analyze to what extent the United States Air Force (USAF) security policies address this problem. The policies are reviewed in terms of how well they align with best practices published by Carnegie Mellon University and additional factors this research deems important, including motivations, organizational priorities, and social networks.

This research offers actionable recommendations that the USAF could implement in order to better prevent, detect, and respond to insider attacks. The most important course of action is to better utilize its workforce. All personnel should be trained on observable behaviors that can be precursors to malicious activity. Additionally, supervisors need to be the first line of defense, monitoring for stress, unmet expectations, and disgruntlement. This research also proposes three new best practices regarding screening for prior concerning behaviors, predispositions, and technical incidents; issuing sanctions for inappropriate technical acts; and requiring supervisors to take a proactive role.

15. SUBJECT TERMS

insider threat, insider attacks, malicious insiders, sabotage, espionage

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Dr. Robert F. Mills (ENG) robert.mills@afit.edu
REPORT	ABSTRACT	c. THIS PAGE			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U	U U	162	(937) 255-3636 x4527; robert.mills@afit.edu